

# EnCase Forensic Version 6.11

## User's Guide



Copyright © 2008 Guidance Software, Inc. All rights reserved.

EnCase®, EnScript®, FastBloc®, Guidance Software® and EnCE® are registered trademarks or trademarks owned by Guidance Software in the United States and other jurisdictions and may not be used without prior written permission. All other marks and brands may be claimed as the property of their respective owners.

No part of this document may be copied or reproduced without the written permission of Guidance Software, Inc. Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation into the owners' benefit, without intent to infringe. Any use and duplication of this material is subject to the terms of the license agreement between you and Guidance Software, Inc. Except as stated in the license agreement or as otherwise permitted under Sections 107 or 108 of the 1976 United States Copyright Act, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise. Product manuals and documentation are specific to the software versions for which they are written. For previous or outdated manuals, product release information, contact Guidance Software, Inc. at <http://www.guidancesoftware.com>. Specifications and information contained in this manual are furnished for informational use only, and are subject to change at any time without notice.

# Contents

<b>CHAPTER 1 Introduction</b>	<b>15</b>
Introduction.....	16
<b>CHAPTER 2 New Features</b>	<b>17</b>
LEF EFS Encryption Enhancement.....	18
WinEn.....	18
Snapshot to DB Module Set.....	19
Lotus Notes Local Database Encryption.....	19
EnCase Examiner Support for Microsoft Vista.....	19
64-Bit EnCase Servlet.....	19
Send to HBGary Responder EnScript .....	20
<b>CHAPTER 3 Installing EnCase Forensic</b>	<b>21</b>
The EnCase Installer .....	22
Minimum Requirements .....	22
Installing the Examiner.....	23
Installed Files .....	25
Uninstalling the Examiner .....	26
Reinstalling the Examiner .....	28
Installing Security Keys .....	29
Troubleshooting Security Keys.....	29
Obtaining Updates.....	30
Configuring Your EnCase Application.....	30
Case Options Tab .....	32
Global Tab .....	33
Color Tab .....	35
Fonts Tab of the Options Dialog .....	36
EnScript Tab.....	38
Storage Paths Tab.....	39
Sharing Configuration Files.....	40
Vista Examiner Support.....	40
Disabling Microsoft Windows Vista User Account Control .....	41
Running a 32-bit Application on a 64-bit Platform .....	43
<b>CHAPTER 4 Using LinEn</b>	<b>45</b>
Introduction.....	46
Viewing the License for LinEn.....	46
Creating a LinEn Boot Disc.....	47
Configuring Your Linux Distribution.....	48
Obtaining a Linux Distribution .....	48

LinEn Set Up Under SUSE .....	49
LinEn Set Up Under Red Hat .....	49
Performing Acquisitions with LinEn .....	50
Setup for a Drive-to-Drive Acquisition .....	50
Doing a Drive-to-Drive Acquisition Using LinEn .....	51
Acquiring Device Configuration Overlays (DCO) and Host Protected Areas (HPA) .....	54
Acquiring a Disk Running in Direct ATA Mode .....	54
Mode Selection.....	55
Doing a Crossover Cable Preview or Acquisition .....	56
Hashing the Subject Drive Using LinEn .....	58
 <b>CHAPTER 5 Navigating the EnCase Interface</b> .....	<b>59</b>
The Main Window .....	60
System Menu .....	61
File Menu.....	62
Edit Menu.....	63
Copy/UnErase.....	64
View Menu.....	66
The Tree Pane and its Tab and Sub-Tab Menus.....	70
The Table Pane and its Tab Bar and View Menu.....	71
Table Pane Menu .....	72
The View Pane and its Tab Bar and View Menu .....	73
View Pane Menu .....	74
The Filter Pane and its Tab Bar and View Menu .....	75
Filter Pane Menu .....	76
Auto Fit.....	76
Tools Menu.....	77
Help Menu .....	78
Toolbar .....	80
Panes .....	82
Panes in the Analysis Cycle .....	83
Panes as Separate Windows .....	84
Pane Features.....	86
Pane Tab Bar and Pane Tab Bar Menu .....	87
Tab Right-Click Menu .....	88
Individual Panes.....	88
Tree Pane .....	89
Table Pane .....	91
Sorting a Table .....	92
Filters Pane.....	93
Filtering Effects in Table Pane .....	94
View Pane.....	96
Status Line.....	96
Panes and their Specific Tabs .....	98
Tree Pane Tabs.....	99
Table Pane Tabs.....	99
Table Tab Columns .....	102



Filters Pane Menu.....	105
View Pane Tabs .....	106
The Text Tab.....	109
The Hex Tab .....	110
The Doc Tab .....	111
The Transcript Tab .....	112
The Picture Tab.....	112
The Report Tab .....	113
The Console Tab .....	114
The Details Tab .....	114
The Output Tab .....	115
Navigating the Tree Pane .....	115
Opening and Closing Folders with Expand/Contract.....	116
Expand All.....	116
Contract All.....	117
Displaying Tree Entry Information for One Branch.....	118
Displaying Expanded Tree Entry Information.....	119
Selecting Tree Entries for Operations.....	120
Using the Dixon Box .....	121
Modifying the Table Pane.....	122
Showing Columns.....	123
Hiding Columns.....	125
Auto Fit All Columns .....	125
Fitting Columns to Data .....	125
Resetting Columns.....	126
Setting a Lock on Columns .....	126
Excluding Search Hits.....	127
Deleting Items.....	128
Filters.....	129
Creating a Filter .....	130
Editing a Filter .....	131
Running a Filter.....	132
Combining Filters.....	134
AND/OR Filter Logic.....	135
Changing Filter Order .....	135
Turning Filters Off .....	136
Deleting a Filter .....	137
Importing Filters.....	137
Exporting Filters.....	137
Conditions.....	138
Creating Conditions.....	139
Editing Conditions.....	141
Running Conditions.....	142
Importing Conditions.....	143
Exporting Conditions .....	144
Queries.....	145
Gallery Tab.....	146

Viewing More Columns .....	146
Viewing Fewer Columns.....	146
Viewing More Rows .....	147
Viewing Fewer Rows.....	147
Timeline Tab .....	147
Modifying the View Pane .....	148
Copy.....	148
Goto.....	148
Find .....	149
<b>CHAPTER 6 Case Management</b>	<b>151</b>
Overview of Case Structure.....	152
Case Management.....	152
Concurrent Case Management.....	153
Indexing a Case .....	153
Case File Format.....	154
Case Backup.....	155
The Options Dialog.....	155
Case Related Features .....	157
Logon Wizard .....	158
Logon Wizard Users Page.....	159
Users Right-Click Menu .....	159
Browse for Folder Dialog .....	160
SAFE Page of the Logon Wizard.....	161
SAFE Right-Click Menu .....	161
Browse for Folder Dialog .....	162
Edit SAFE Dialog.....	163
New Case Wizard.....	166
Role Page of the New Case Wizard .....	167
Case Options Page of the New Case Wizard.....	168
Add Device.....	168
Using a Case .....	169
Modifying Case Related Settings.....	169
Time Zone Settings.....	170
Case File Time Zones .....	171
Evidence File Time Zones .....	172
Setting Time Zones Settings for Case Files .....	172
Setting Time Zone Options for Evidence Files.....	173
General Time Zone Notes .....	174
FAT, HFS and CDFS Time Zone Specifics .....	174
Time Zone Example .....	175
Open a Case.....	175
Saving a Case.....	176
Saving a Case .....	176
Saving a Case With a New Name or New Location.....	176
Saving a Case and the Global Application Files .....	177
Close Case .....	177

---

**CHAPTER 7 Working with Evidence** **179**


---

Overview .....	180
Types of Entries .....	180
EnCase Evidence Files .....	180
Logical Evidence Files .....	181
Raw Image Files.....	181
Single Files.....	181
Supported File Systems and Operating Systems.....	182
Using Snapshots.....	182
Getting Ready to Acquire the Content of a Device .....	183
Previewing .....	183
Live Device and FastBloc Indicators.....	184
Previewing the Content of a Device .....	184
Add Device Wizard .....	185
Sources Page of the Add Device Wizard .....	186
Sessions Sources Page of the Add Device Wizard.....	188
Choose Devices Page of the Add Device Wizard .....	190
Preview Devices Page of the Add Device Wizard.....	192
Adding a Device.....	193
Completing the Sources Page .....	194
Completing the Sessions Sources Page .....	195
Completing the Choose Devices Page.....	195
Completing the Preview Devices Page .....	196
Acquiring .....	196
Types of Acquisitions .....	197
Doing a Typical Acquisition .....	197
Acquisition Wizard.....	198
After Acquisition Page .....	199
Search Page .....	201
Options Page.....	204
Acquisition Results Dialog.....	206
Opening the Acquisition Wizard .....	207
Specifying and Running an Acquisition .....	208
Completing the After Acquisition Page of the Acquisition Wizard.....	209
Completing the Search Page of the Acquisition Wizard.....	210
Completing the Options Page of the Acquisition Wizard .....	212
Canceling an Acquisition .....	213
Acquiring a Local Drive .....	214
Acquiring Device Configuration Overlays (DCO) and Host Protected Areas (HPA).....	214
Using a Write Blocker.....	215
Windows-based Acquisitions with FastBloc Write Blockers .....	215
Acquiring in Windows Without a FastBloc Write Blocker.....	217
Windows-based Acquisitions with a non-FastBloc Write Blocker .....	217
Performing a Drive-to-Drive Acquisition Using LinEn .....	218
Acquiring a Disk Running in Direct ATA Mode .....	219
Acquiring a Palm Pilot .....	220

Leaving Console Mode.....	222
Acquisition Times .....	223
Acquiring Non-local Drives.....	223
When to use a Crossover Cable.....	223
Performing a Crossover Cable Preview or Acquisition.....	223
Acquiring Disk Configurations.....	225
Software RAID.....	225
Windows NT - Software Disk Configurations .....	226
Dynamic Disk .....	227
Hardware Disk Configuration .....	228
Disk Configuration Set Acquired as One Drive.....	228
Disk Configurations Acquired as Separate Drives .....	229
Validating Parity on a RAID-5 .....	230
RAID-10 .....	230
Acquiring Virtual PC Images .....	230
CD-DVD Inspector File Support .....	230
Acquiring SlySoft CloneCD Images .....	230
Acquiring a DriveSpace Volume.....	231
Acquiring Firefox Cache in Records.....	232
Reacquiring Evidence.....	233
Reacquiring an Evidence File .....	233
Adding Raw Evidence Files.....	234
Remote Acquisition .....	235
Remote Acquisition Monitor .....	237
Setting Up the Storage Machine .....	238
Hashing.....	240
Hashing the Subject Drive Using LinEn.....	240
Hashing the Subject Drive Once Previewed or Acquired .....	241
Logical Evidence Files.....	242
Create Logical Evidence File Wizard.....	243
Sources Page .....	244
The Outputs Page of the Create Logical Evidence File .....	245
Creating a Logical Evidence File.....	246
Recovering Folders .....	247
Recover Folders on FAT Volumes .....	248
Recovering NTFS Folders.....	248
Recovering UFS and EXT2/3 Partitions.....	250
Recovering Folders from a Formatted Drive.....	250
Recovering Partitions .....	250
Adding Partitions.....	251
Deleting Partitions .....	253
Restoring Evidence .....	254
Physical vs. Logical Restoration.....	254
Preparing the Target Media .....	254
Physical Restore.....	255
Logical Restore .....	258
Bootting the Restored Hard Drive .....	258

If the Restored Disk Does Not Boot .....	259
Snapshot to DB Module Set .....	260
Initializing the Database .....	260
Choosing Database Sources .....	261
Maintaining the Database .....	262
Updating the Database .....	263
Specifying Database Content .....	265
Generating Reports on the Database .....	266
Using the Snapshot DB Reports Dialog .....	268
WinEn .....	270
Running WinEn .....	271
Command Line Options .....	272
Configuration File .....	273
Configuration File Notes .....	274
Prompt for Value .....	274
Error Handling .....	274
Additional WinEn Information .....	274
<b>CHAPTER 8 Viewing File Content .....</b>	<b>277</b>
Viewing Files .....	278
Copying and Unerasing Files and Folders .....	279
Copy and Unerase Features .....	279
Copy/UnErase Wizard .....	280
File Selection Page of the Copy/UnErase Wizard .....	281
Options Page of the Copy/UnErase Wizard .....	283
Destination Page of the Copy/UnErase Wizard .....	285
Copy Folders Dialog .....	286
Copying and Unerasing Files .....	288
Completing the File Selection Page .....	289
Completing the Options Page .....	290
Completing the Destination Page .....	290
Copying and Unerasing Bookmarks .....	290
Copying Folders .....	291
File Viewers .....	292
File Viewer Features .....	292
New File Viewer Dialog .....	293
Viewer File Type Dialog .....	293
Adding a File Viewer to Your EnCase Application .....	294
Associating the File Viewer's File Types with the Viewer .....	295
View Pane .....	296
Viewing Compound Files .....	297
Viewing File Structure .....	297
Viewing Registry Files .....	299
Viewing OLE Files .....	301
Viewing Compressed Files .....	302
Viewing Lotus Notes Files .....	303
Viewing MS Exchange Files .....	303

Exchange Server Synchronization.....	303
Cleaning an EDB Database .....	304
Testing an EDB File.....	305
Recovering a Database.....	306
Repairing a Database .....	306
Viewing Outlook Express Email .....	307
Viewing MS Outlook Email .....	310
Viewing Macintosh .pax Files.....	311
Viewing Windows Thumbs.db .....	313
America Online .art Files.....	314
Viewing Office 2007 Documents .....	315
Viewing Base64 and UUE Encoded Files .....	316
NTFS Compressed Files .....	318
Gallery Tab .....	318
Bookmarking an Image .....	319
Reducing the Number of Images Per Row .....	320
Increasing the Number of Images Per Row .....	320
Clearing the Invalid Image Cache.....	321
Lotus Notes Local Encryption Support .....	321
Determining Local Mailbox Encryption.....	322
Parsing a Locally Encrypted Mailbox.....	322
Encrypted Block .....	323
Decrypted Block .....	324
Locally Encrypted NSF Parsing Results.....	325
<b>CHAPTER 9 Analyzing and Searching Files</b> .....	<b>327</b>
Signature Analysis .....	328
File Signatures .....	328
File Signatures with Suffixes.....	329
Viewing the File Signature Directory .....	329
Adding a New File Signature .....	331
Editing a Signature.....	332
Performing a Signature Analysis .....	333
Viewing Signature Analysis Results (Part 1).....	334
Viewing Signature Analysis Results (Part 2).....	335
Signature Analysis Legend .....	336
EnScript Programming Language .....	337
Included Enscript Components.....	337
EnScript Types.....	338
Hash Analysis.....	338
File Hashing.....	339
Hash a New Case .....	339
Hash Sets.....	340
Create a Hash Set .....	340
Rebuild a Hash Library .....	342
Viewing Hash Search Results .....	342
Keyword Searches .....	343

Creating Global Keywords .....	344
Adding Keywords.....	344
Creating International Keywords .....	347
Keyword Tester .....	348
Local Keywords.....	350
Import Keywords .....	350
Export Keywords .....	350
Searching Entries for Email and Internet Artifacts.....	352
Internet History Searching.....	355
Comprehensive Internet History Search.....	355
Internet Searching .....	356
Performing a Search.....	357
Search Options.....	357
Viewing Record Search Hits .....	359
Viewing Search Hits.....	360
Exclude Files .....	360
Show Excluded Files .....	361
Deleting Items.....	362
Show Deleted Files.....	363
Encode Preview.....	363
Turning On Encode Preview .....	363
Indexing .....	365
Querying an Index Using a Condition .....	366
Generating an Index .....	367
Searching for Email.....	369
Web Mail Parser .....	370
Extracting Email .....	371
Searching Email.....	372
Searching Selected Items .....	373
Viewing Attachments .....	374
Export to *.msg .....	375
Exporting to *.msg.....	376
App Descriptors .....	378
Manually Create App Descriptor.....	378
Create an App Descriptor with an EnScript Program.....	380
Encryption Support .....	381
NSF Encryption Support .....	382
Recovering NSF Passwords .....	383
Disk Encryption Support.....	384
SafeBoot Setup .....	385
Exporting a Machine Profile from the SafeBoot Server .....	386
Authentication.....	387
SafeBoot Encryption Support (Disk Encryption).....	387
Supported SafeBoot Encryption Algorithms.....	390
CREDANT Encryption Support (File-Based Encryption) .....	390
Supported Encryption Algorithms .....	393
CREDANT Encryption Support (Offline Scenario) .....	393

Enabling the Forensic Administrator Role on the CREDANT Server .....	395
S/MIME Encryption Support .....	395
EFS Files and Logical Evidence (LO1) Files .....	399

## CHAPTER 10 Bookmarking Items 401

---

Bookmarks Overview .....	402
Highlighted Data Bookmarks .....	403
Notes Bookmarks .....	403
Folder Information/Structure Bookmarks .....	404
Notable File Bookmarks .....	404
File Group Bookmarks .....	404
Snapshot Bookmarks .....	405
Log Record Bookmarks .....	405
Datamarks .....	406
Bookmark Features .....	406
Bookmark Data Dialog for Highlighted Data Bookmarks .....	407
Bookmark Content Data Types .....	407
Text .....	408
Picture .....	408
Integers .....	409
Dates .....	409
Windows .....	410
Styles .....	410
Add Note Bookmark Dialog .....	411
Bookmark Folder Information/Structure Dialog .....	412
Bookmark Data Dialog for Files .....	413
Creating a Bookmark .....	414
Creating a Highlighted Data Bookmark .....	415
Creating a Notes Bookmark .....	416
Creating a Folder Information/Structure Bookmark .....	417
Creating a Notable File Bookmark .....	418
Creating a File Group Bookmark .....	419
Creating a Log Record Bookmark .....	420
Creating a Snapshot Bookmark .....	421
Creating a Datamark as a Bookmark .....	422
Using Bookmarks .....	422
Editing a Bookmark .....	423
Bookmark Editing Dialogs .....	424
Edit Highlighted Data Bookmarks Dialog .....	425
Edit Note Bookmarks Dialog .....	426
Edit Folder Information/Structure Bookmarks Dialog .....	426
Edit Notable File Bookmarks Dialog .....	427
Edit Snapshot Bookmarks Dialog .....	427
Edit Log Record Bookmarks Dialog .....	428
Edit Datamarks Dialog .....	428
Edit Bookmark Folder Dialogs .....	429
Edit Folder Dialog .....	430



Using a Folder to Organize a Bookmarks Report .....	431
Organizing Bookmarks.....	432
Copying a Table Entry into a Folder.....	433
Moving a Table Entry into a Folder Using the Right-Click Drag Method .....	434
Moving a Table Entry or Folder into a Folder Using the Drag Method .....	435
Bookmark Reports and Reporting .....	435
Viewing a Bookmark on the Table Report Tab .....	436
Customizing a Report.....	437
Excluding Bookmarks.....	438
Exclude File Bookmarks .....	438
Exclude Folder.....	439
Show Excluded .....	441
<b>CHAPTER 11 Reporting</b>	<b>443</b>
Reporting .....	444
Creating a Report Using the Report Tab .....	444
Enabling or Disabling Entries in the Report.....	445
Report Single Files.....	445
Report Multiple Files .....	446
Changing Report Size .....	447
Viewing a Bookmark Report .....	447
Email Report .....	448
Internet Report.....	449
Creating a Webmail Report .....	449
Alternative Report Method.....	450
Search Hits Report .....	451
Quick Entry Report .....	453
Creating an Additional Fields Report .....	454
Exporting a Report.....	455
Creating a Report Using Case Processor .....	456
<b>CHAPTER 12 Working with Non-English Languages</b>	<b>457</b>
Working with Non-English Languages .....	458
Non-English Language Features .....	459
The Options Dialog Font Tab .....	460
Unicode Fonts .....	461
Text Styles .....	461
New Text Styles Dialog .....	462
New Text Styles Dialog Attributes Tab.....	462
New Text Styles Dialog Code Page Tab.....	464
Configuring Non-English Language Support .....	465
Configuring Interface Elements to Display Non-English Characters .....	466
Configuring the Keyboard for a Specific Non-English Language.....	467
Entering Non-English Content without Using Non-English Keyboard Mapping.....	468
Creating and Defining a New Text Style .....	469
Creating Non-English Keywords.....	471

Testing a Non-English Keyword.....	473
Querying the Index for Non-English Content.....	474
Bookmarking Non-English Language Text .....	475
Viewing Unicode Files.....	476
Viewing Non-Unicode Files.....	477
Associating Code Pages.....	477
<b>CHAPTER 13 EnScript Analysis</b>	<b>479</b>
EnScript Analysis.....	480
Enterprise EnScript Programs.....	481
Document Incident.....	482
Machine Survey Servlet Deploy .....	484
Quick Snapshot.....	488
Remote Acquisition Monitor .....	488
Snapshot Differential Report .....	489
Sweep Enterprise.....	490
Forensic EnScript Code .....	491
Case Processor .....	492
Case Processor Modules.....	494
File Mounter.....	495
Compound Files .....	497
Mounting Compound Files.....	497
Index Case .....	497
Scan Local Machine.....	498
Webmail Parser.....	498
EnScript Example Code .....	499
COM Folder EnScript Code .....	499
EnScript Debugger.....	500
Help for EnScript Modules .....	502
EnScript File Mounter.....	503
Include EnScript .....	504
EnScript Help.....	505
EnScript Types.....	505
Packages .....	505
Package Features .....	505
New Package Dialog.....	506
Package Panel .....	506
Properties Panel.....	507
Create License Dialog .....	508
Using a Package.....	509
Creating a Package.....	509
Editing a Package .....	510
Building a Package.....	510
Creating a License .....	510
Running a Package.....	511
Send To HBGary Responder EnScript .....	511

<b>CHAPTER 14 Using EnCase Tools</b>	<b>515</b>
Toolbar .....	516
Tools Menu .....	517
EnScript Programs Shortcut Submenu.....	518
Wipe Drive .....	518
Verifying Evidence Files.....	521
Creating a LinEn Boot Disc.....	522
Options .....	523
<b>CHAPTER 15 Glossary of Terms</b>	<b>525</b>
<b>CHAPTER 16 Guidance Software</b>	<b>535</b>
Legal Notification .....	536
Support.....	537
Reference Manuals and Release Notes.....	537
Technical Support .....	538
Customer Service.....	543
Training .....	543
Professional Services.....	544
<b>Index</b>	<b>545</b>



# Introduction

■	Introduction	15
---	--------------	----

## Introduction

Thank you for purchasing your Guidance Software application. You now own the world's leading technology for computer and enterprise investigation. This application is just one of the many court-validated Guidance Software solutions used by government agencies, corporate organizations, and law enforcement investigators around the world.

Guidance Software solutions provide an enterprise investigative infrastructure that enables corporations, government and law enforcement agencies to conduct effective digital investigations, respond promptly to large-scale data collection needs, and take decisive action in response to external attacks.

Guidance Software products have changed the landscape by providing complete, immediate response and comprehensive, forensic-level analysis of information found anywhere on a computer. These products are scalable platforms that integrate seamlessly with existing systems to create an investigative infrastructure.

# New Features

- LEF EFS Encryption Enhancement 17
- WinEn 18
- Snapshot to DB Module Set 19
- Lotus Notes Local Database Encryption 19
- EnCase Examiner Support for Microsoft Vista 19
- 64-Bit EnCase Servlet 19
- Send to HBGary Responder EnScript 20

## LEF EFS Encryption Enhancement

There were different scenarios from previous EnCase versions for adding EFS files to a logical evidence (L01) case:

1. The file is *encrypted* and the *\$EFS stream is missing from the same folder* within the L01: **the file cannot be decrypted.**
2. The file is *encrypted* and the *\$EFS stream is in the same folder*: **the file can be decrypted** (except for the remainder of the file, if any).
3. The file is *decrypted* and the *\$EFS stream is in the same folder*: **the file will be decrypted twice.** The file is *decrypted* and the *\$EFS stream is missing*: **the file remains decrypted.**
4. The file is *decrypted* and the *\$EFS stream is in the same folder*: **the file will be decrypted twice.**

All of the above scenarios are now handled gracefully because the \$EFS stream is added internally.

## WinEn

WinEn is a standalone command line utility that captures the physical memory on a live computer running a Windows operating system (Windows 2000 or higher). The physical memory image captured by WinEn is placed in a standard evidence file, along with the user-supplied options and information.

WinEn runs from a command prompt on the computer where you want to capture the memory. WinEn has a very small footprint in memory, and it is typically run from a removable device such as a thumb drive. Although this method makes minor changes to the computer running WinEn, this is the most effective way to capture physical memory before shutting down a computer.



## Snapshot to DB Module Set

This script takes snapshots of nodes across a network and stores the snapshots in a SQL database. It also reads from the database to create reports on the snapshots taken. It allows for minimal maintenance on the database so that you can control the amount of data stored.

Three EnScripts work with the database to perform their tasks:

- Initialize Database.EnScript
- Snapshot to DB.EnScript
- Snapshot DB Reports.EnScript

## Lotus Notes Local Database Encryption

EnCase can now decrypt a local Lotus Notes user mailbox (NSF file suffix). The local mailbox is a replica of the corresponding encrypted mailbox on the Domino server.

## EnCase Examiner Support for Microsoft Vista

EnCase Examiner now supports the Windows Vista operating system.

EnCase must run as an administrator to access the local Vista computer.

## 64-Bit EnCase Servlet

EnCase now includes a servlet for the 64-bit versions of Windows XP, 2003, and Vista operating systems.

---

If not installed as a service, you must Run as Administrator.

---

## Send to HBGary Responder EnScript

This EnScript passes a memory object gathered by EnCase to HBGary's Responder software. EnScript drops the physical evidence device information, byte for byte, into a flat file and sends it to Responder.

# Installing EnCase Forensic

- The EnCase Installer 21
- Installing Security Keys 29
- Troubleshooting Security Keys 29
- Obtaining Updates 30
- Configuring Your EnCase Application 30
- Sharing Configuration Files 40
- Vista Examiner Support 40
- Running a 32-bit Application on a 64-bit Platform 43

## The EnCase Installer

The EnCase installer copies the program and its drivers to the end user's computer or client and initializes drivers and services with the operating system.

The investigator can select where to install the EnCase Examiner. The default is the Program Files folder. If a selected directory exists, the installer overwrites any existing program files, logs, and drivers.

## Minimum Requirements

For best performance, examination computers should be configured with at least the following hardware and software:

- An EnCase security key (also known as a dongle)
- Certificates for all purchased modules (known as certs)
- A current version of EnCase Examiner
- Pentium IV 1.4 GHz or faster processor
- One GB of RAM
- Windows 2000, XP Professional, or 2003 Server
- 55 MB of free hard drive space

The program also supports the 64-bit version of Windows.

---

Note: Intel Itanium processors are not supported.

---

---

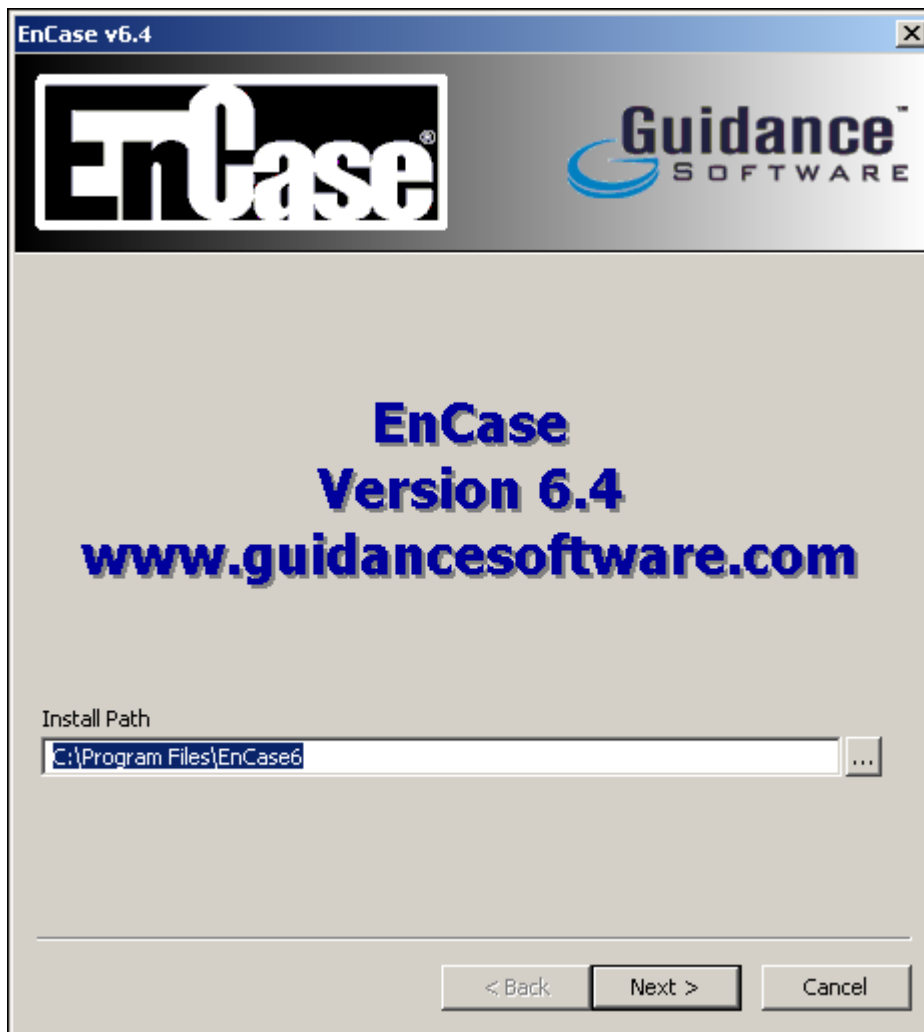
Note: FastBloc SE supports only the USB interface with the 64-bit version.

---

## Installing the Examiner

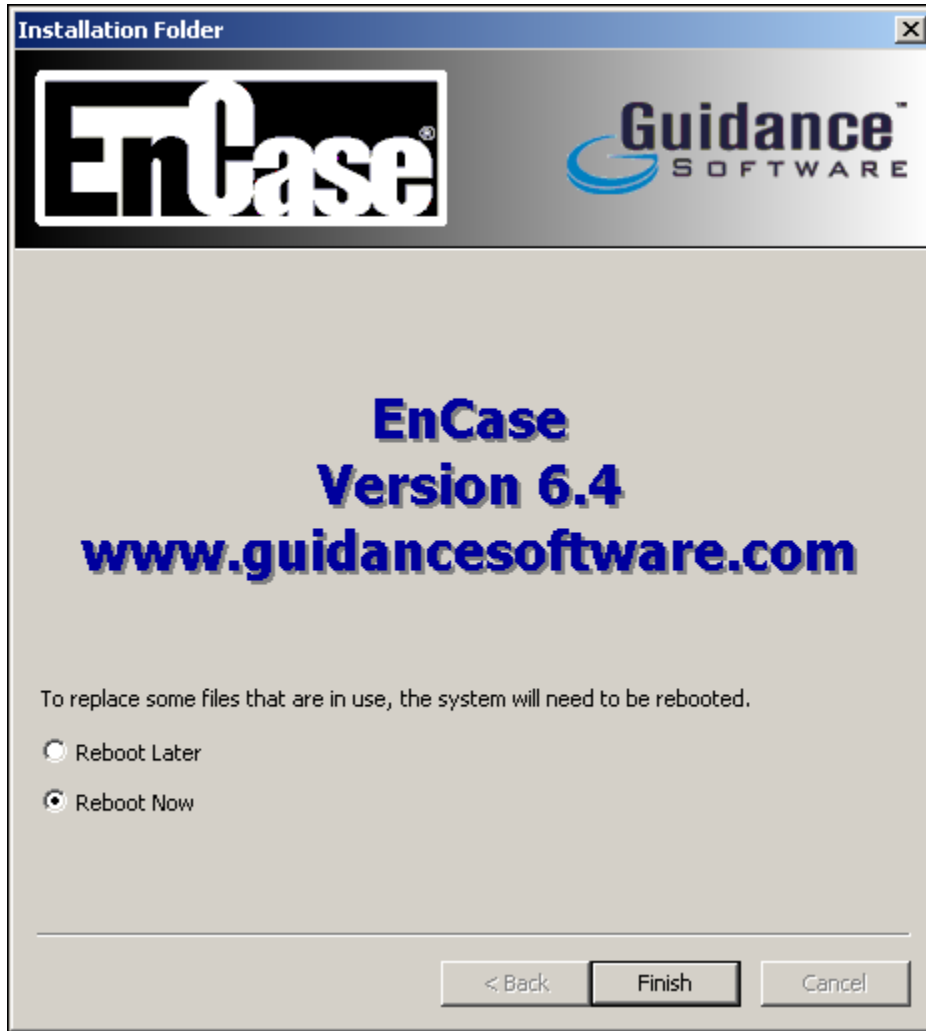
If you are using Local Processing, install the program by inserting the CD into a player and waiting for autostart. Do this for each client. If are using Terminal Services, install the program using the Add/Remove programs wizard on the application server.

Once installation begins, a wizard displays:



Note: C:\Program Files\EnCase6 is the install path default.

1. Enter an installation path or accept the default and click **Next**.
2. Read and agree with the EnCase License Agreement and click **Next**.
3. Click **Next**



4. Select **Reboot Later** or **Reboot Now** and click **Finish**.

## Installed Files

During installation, the program copies itself and a collection of associated files to the target directory.

The installer places a startup icon on the desktop. In addition, a number of folders and files are installed in the target folder during installation.

### Certs Folder

- EnCase.pcert

### Config Folder

- AppDescriptors.ini
- FileSignatures.ini
- FileTypes.ini
- Filters.ini
- Keywords.ini
- Profiles.ini
- TextStyles.ini

### Storage Folder

- CaseReport.ini
- Compromise Assessment Module.ini
- DifferentialReport.ini
- SweepEnterpriseWEBReport.ini

### Forensic EnScript Component Folder

- Case Processor.EnScript
- File Mounter.EnScript
- Index Case.EnScript
- Scan Local Machine.EnScript
- Webmail Parser.EnScript

## Uninstalling the Examiner

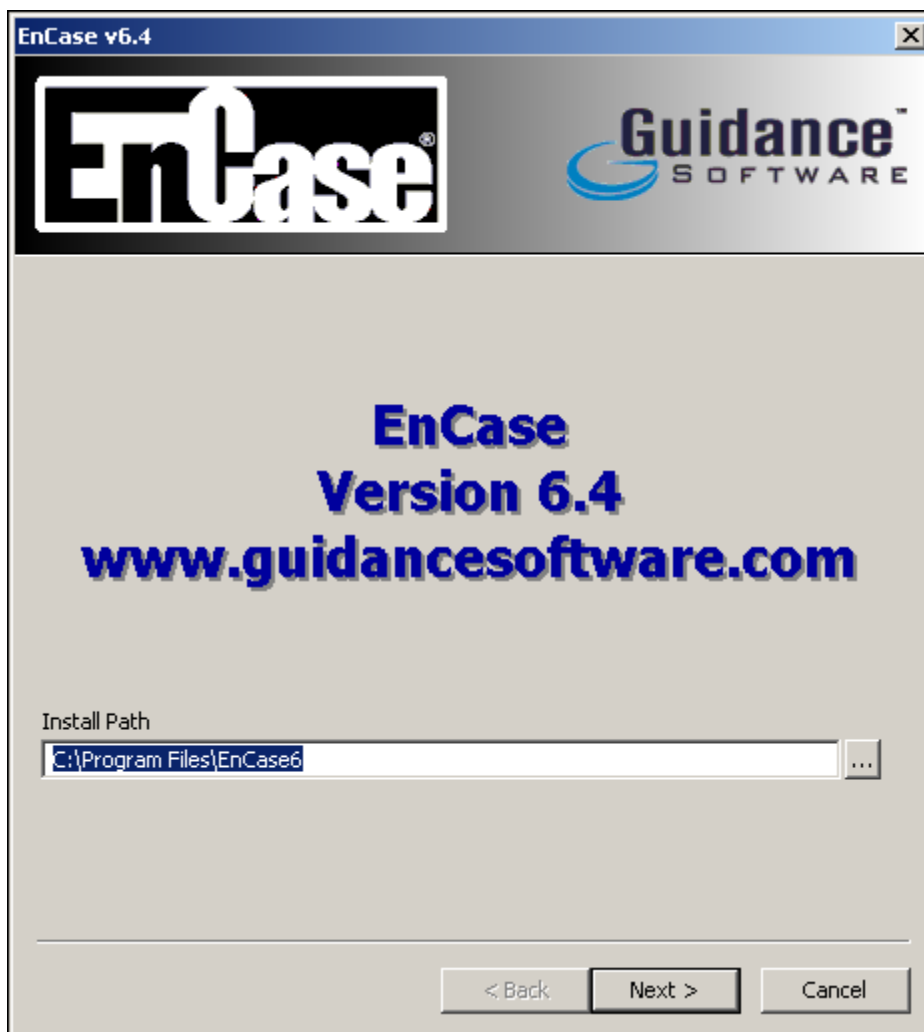
The uninstaller works only on identical software versions.

- Have backups of evidence and case files prior to making any modifications to any software on an examination machine. An update of the program is also required.
- Close any running versions of the EnCase® program, insert the software's installation media and wait for the installer to come online.

1. Open Windows Control Panel and double-click **Change or Remove Programs**.
2. Select the EnCase version being removed and click **Change/Remove**.

The EnCase uninstall wizard runs and the first screen displays

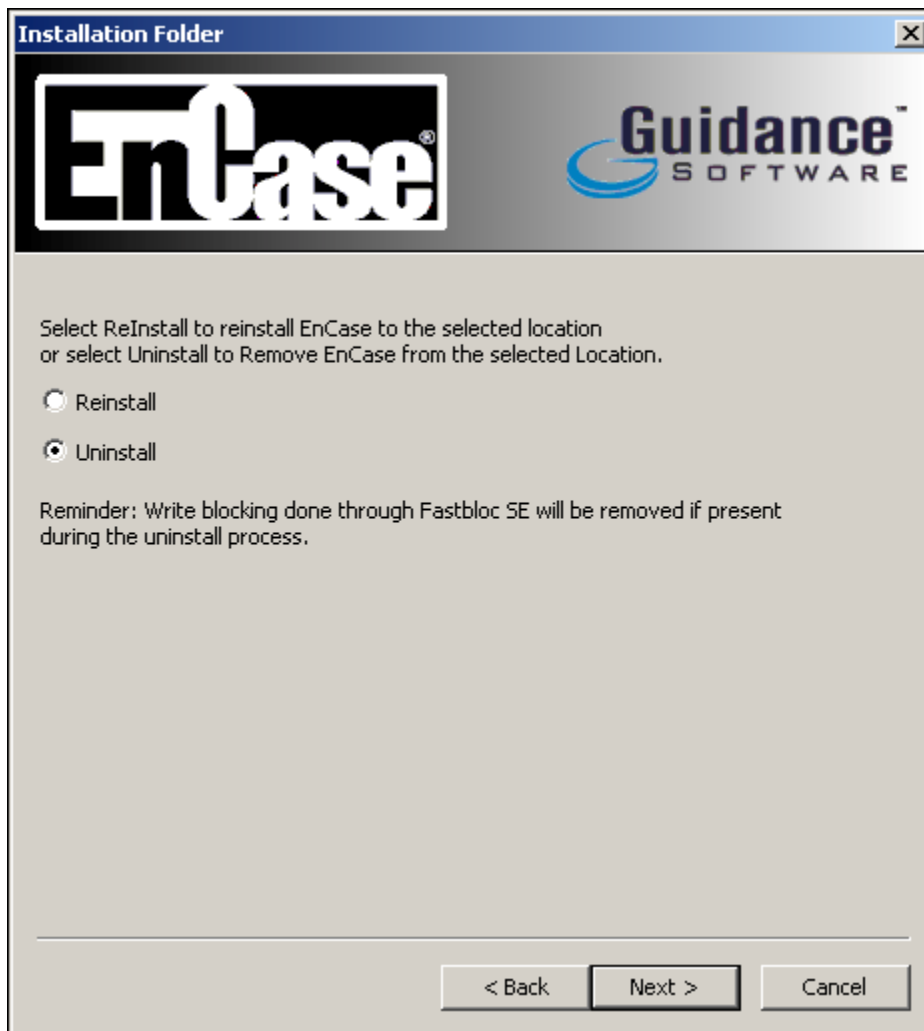
3. Enter or navigate to the software's location in the Install Path field. The default is C:\Program Files\Encase6.
4. Click **Next**. The EnCase uninstall wizard runs.





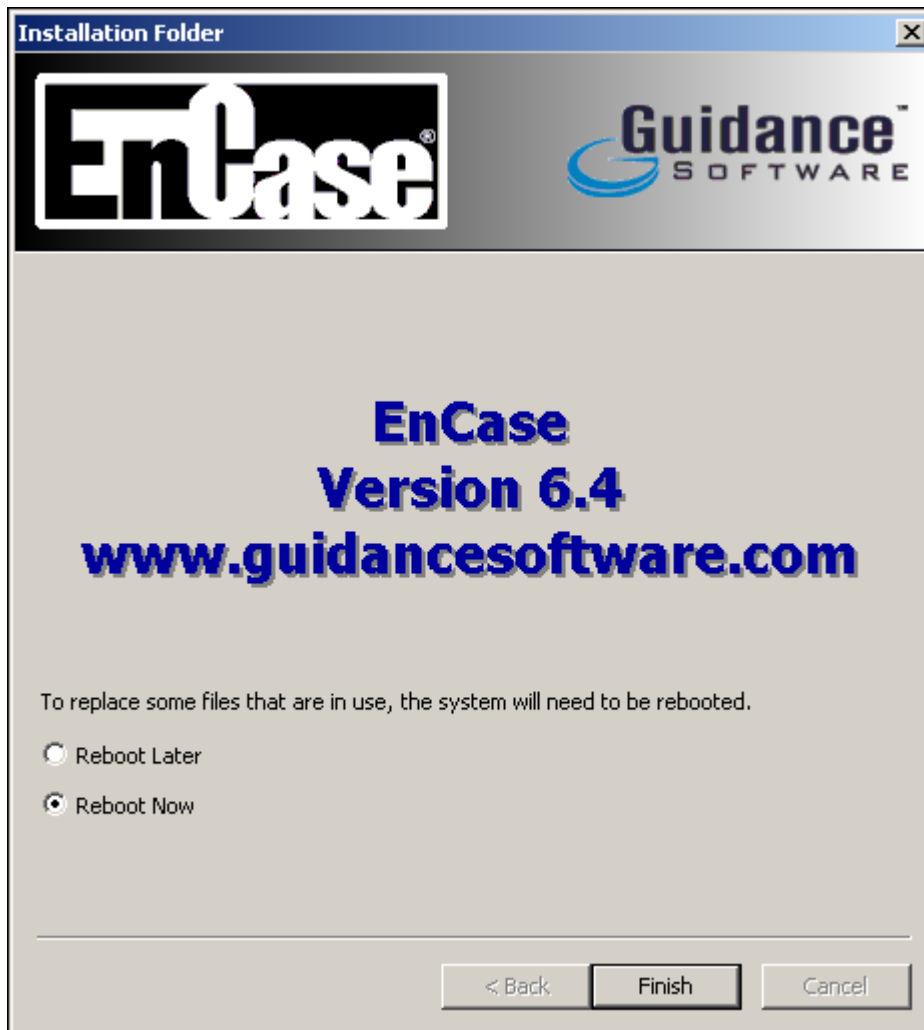
5. Click **Next**.

Page 2 of the uninstall wizard displays.



6. Select **Uninstall** and click **Next**. Progress shows on the dialog.
7. When the completion notification displays, click **Finish**.

Software is removed and page 3 of the uninstall wizard displays.



8. Select **Reboot Later** or **Reboot Now** and click **Finish**.

## Reinstalling the Examiner

---

Note: Reinstall does not overwrite existing user files.

---

Reinstall refreshes certain files and settings and is a variation of the install program.

Reinstall creates a new log file and reinstalls the following items:

- Application files
- Registry keys
- User files that do not exist

## Installing Security Keys

NAS provides licensing to the clients eliminating the need for security keys on client machines, however, you must still install the security key drivers for your SAFE machine.

Before you begin, ensure your EnCase application is closed.

*To install your security keys:*

1. Insert the installation CD-ROM.
2. If autorun is enabled, the splash screen appears.
3. Click the security key drivers link.
4. Click **Next** when HASP installation wizard displays.
5. Click **Next** when the summary displays.
6. Click **Finish** when the installation is complete.
7. Insert the security key and Windows will find the security key.
8. Open the EnCase application.

---

Note: If the security key is inserted before clicking **Finish**, the drivers will not be installed properly. Remedy this condition by reinstalling the driver with the security key removed.

---

## Troubleshooting Security Keys

Installation is usually trouble-free, but if there are problems with installation, go to the troubleshooting page

<http://www.guidancesoftware.com/support/articles/articles.asp>  
(<http://www.guidancesoftware.com/support/articles/articles.asp>) on our Web site.

Navigate to the message board to research your problem.

## Obtaining Updates

Version 6 is the latest and most current version of the software suite. Updates containing new and upgraded features, however, are published on a regular basis.

To protect your chain of custody and to ensure you have the latest updates installed, it is important to ensure the installed program is up to date.

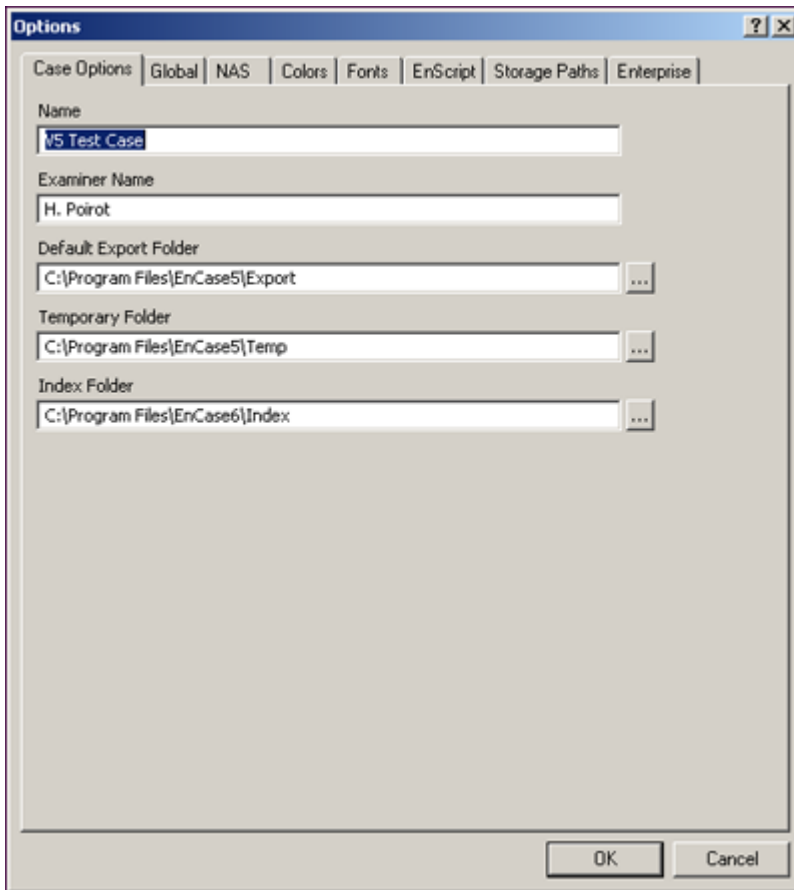
See the Downloads topic in the *EnCase Enterprise Administration Guide* for more information on obtaining software updates.

## Configuring Your EnCase Application

You can configure various aspects of the EnCase application according to your needs or preferences. These settings are used each time you start EnCase. You are not required to open a case. When a case is open, a Cases Options tab displays in the Options dialog.

*To configure EnCase:*

1. Click **Tools > Options**. The Options dialog appears.



2. Click the desired tab and change the settings as needed, then click **OK**.

---

Note: Some changes made to the options settings take effect when you restart EnCase. Some take effect immediately.

---

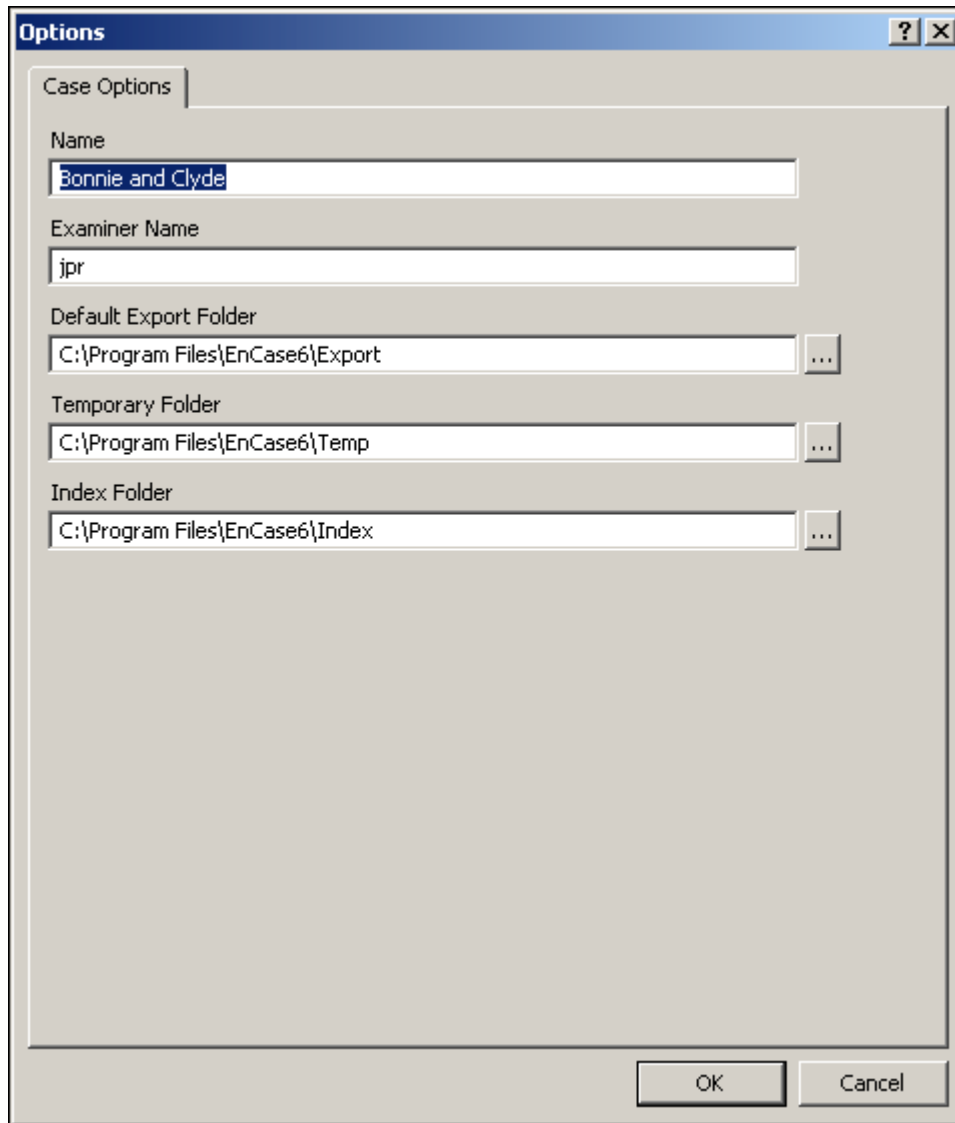
The Options dialog contains the following tabs:

- ☐ Case Options
- ☐ Global
- ☐ Colors
- ☐ Fonts
- ☐ EnScript Programs
- ☐ Storage Paths

The Case Options tab displays only when a case is open.

## Case Options Tab

The Case Options tab contains settings that apply to the open case.



**Name** contains the name of the case associated with the case options set on this tab. The case name is used as the default filename when the case is saved. The filename can be changed when the file is saved.

**Examiner Name** contains the name of the user acting as the investigator.

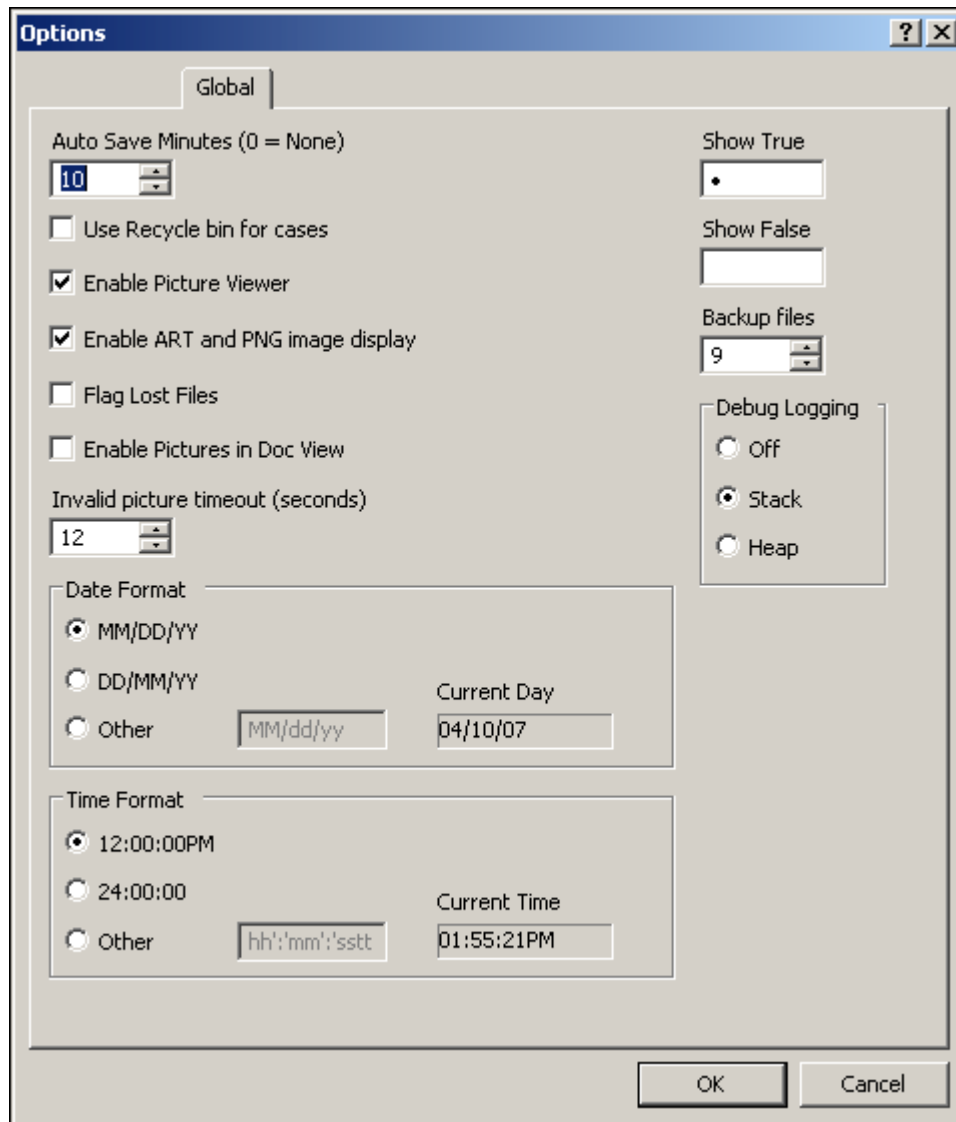
**Default Export Folder** contains the path and name of the folder where files are exported.

**Temporary Folder** contains the path and name of the folder where temporary files are created.

**Index Folder** contains the index file for any indexed file or collection of files.

## Global Tab

The Global tab of the Options dialog contains settings that apply to all cases.



**Auto Save Minutes (0 = None)** contains the number of minutes that constitute the interval between automatic saves of case files. The automatically saved data is written to \*.CBAK files.

**Use Recycle Bin for Cases** determines whether backup files are moved to the recycle bin and not overwritten when a file is automatically saved.

**Enable Picture Viewer** determines whether the picture viewer is used for graphics of the appropriate formats.

**Enable ART and PNG Image Display** determines whether ART and PNG image files are displayed. When these files are corrupted, they can cause the program to crash, so this setting enables you to limit the impact of corrupted ART and PNG files.

**Flag Lost Files** determines whether lost clusters are treated as unallocated space. Doing so decreases the amount of time required to access the evidence file. When selected, all lost clusters appear in the disk tab as unallocated clusters.

**Enable Pictures in Doc View** determines whether pictures that are natively displayed by EnCase display using Oracle Outside In technology in the Doc tab of the View pane.

**Invalid Picture Timeout (seconds)** contains the amount of time the program attempts to read a corrupt image file before timing out. When the read times out, the corrupt file is sent to the cache and no attempt is made to read it again.

**Date Format** includes these options:

- **MM/DD/YY** (for example, 06/21/08)
- **DD/MM/YY** (for example, 21/06/08)
- **Other** enables you to specify your own date format.
- **Current Day** contains the current date in the specified date format.

**Time Format** includes these options:

- **12:00:00PM** determines whether a twelve-hour clock is the basis of the time format.
- **24:00:00** determines whether a twenty-four hour clock is the basis of the time format.
- **Other** enables you to specify your own time format.
- **Current Time** contains the current time in the time format selected.

**Show True** contains the symbol indicating a value of *true* in table columns displayed in the Table tab of the Table pane.

**Show False** contains the symbol used indicating a value of *false* in table columns displayed in the Table tab of the Table pane.



**Backup Files** contain the maximum number of files stored as backup files when a case is saved.

**Debug Logging** contains the various settings that determine where debugging is logged.

## Color Tab

This tab enables you to associate colors with various case elements.

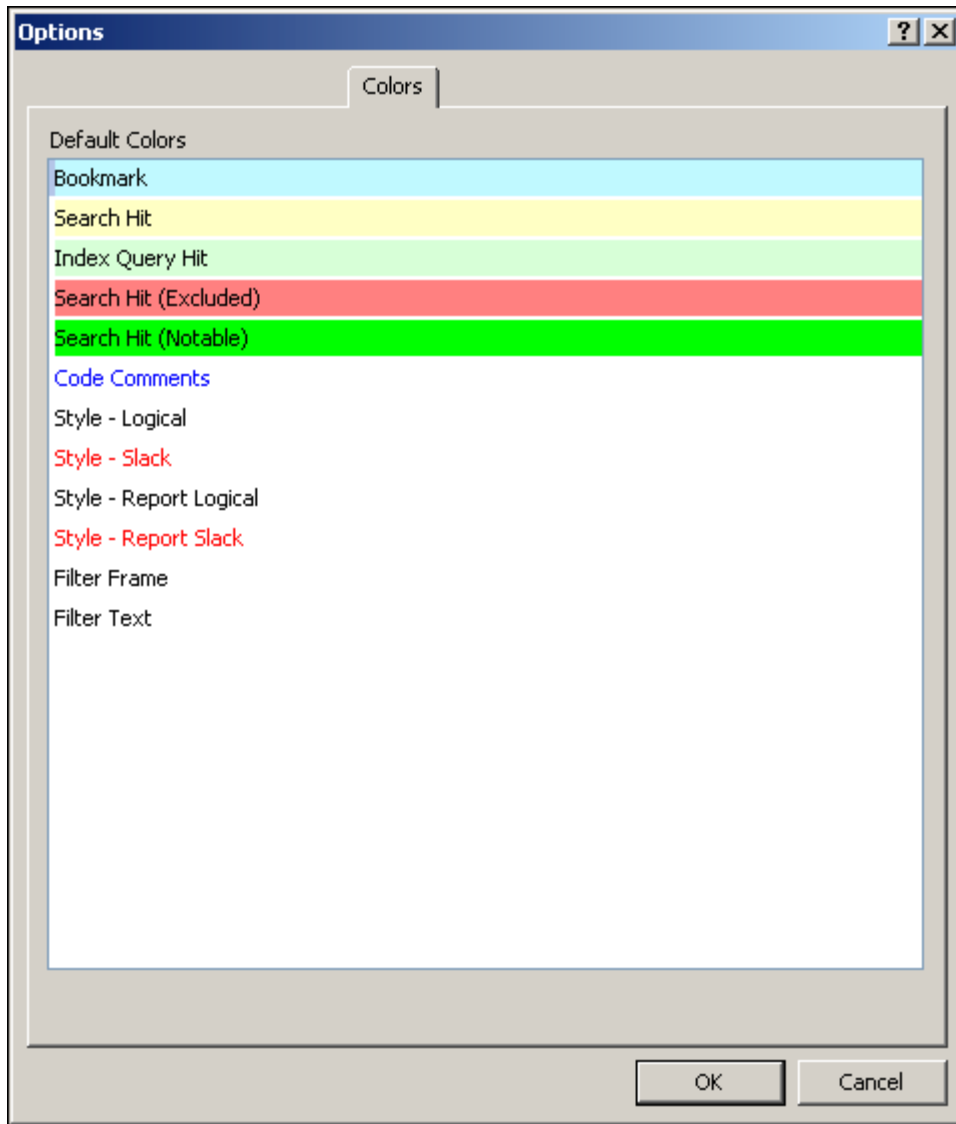
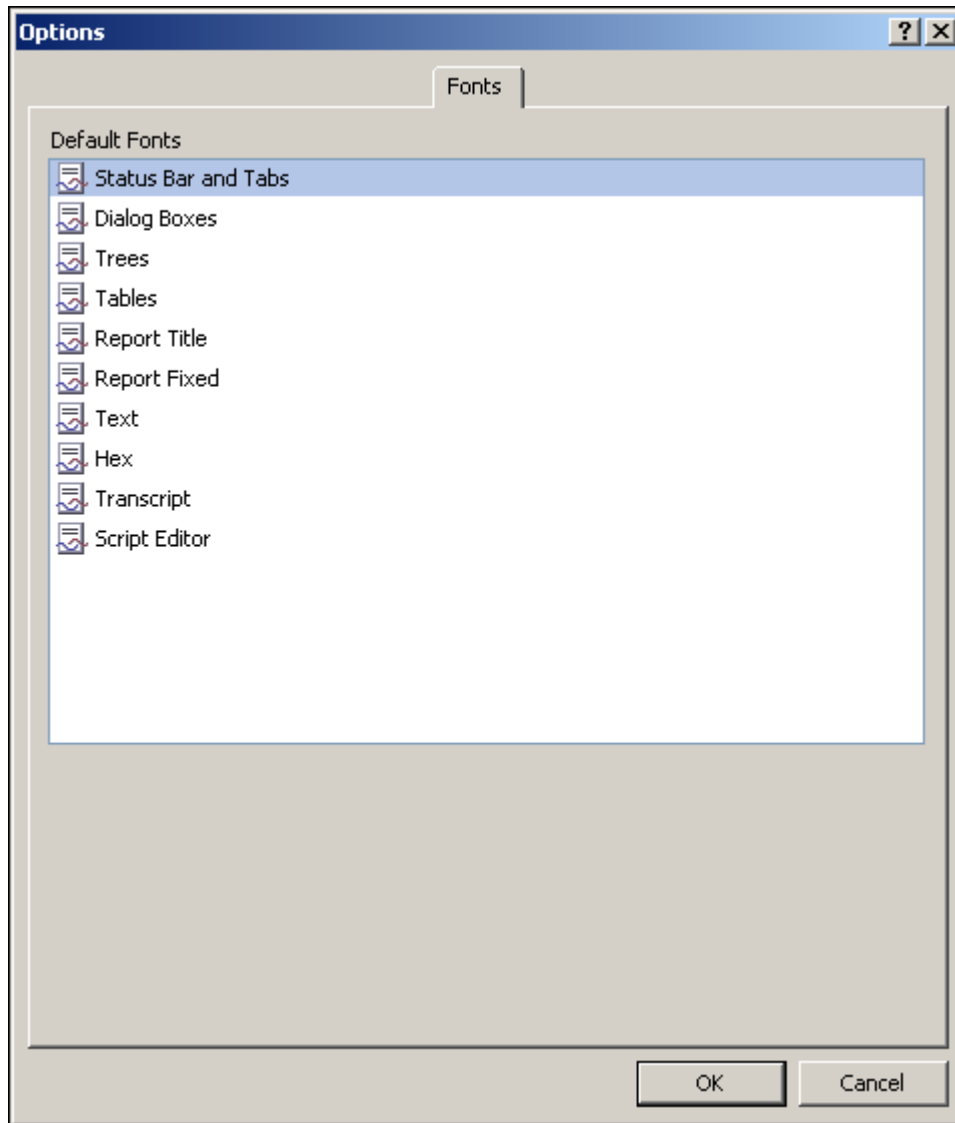


Figure 2

**Default Colors** contains a list of case elements that can be associated with a color. Double clicking on a listed element opens the Color Palette dialog so you can choose and associate a color with the listed case element.

## Fonts Tab of the Options Dialog

This tab enables you to associate fonts with various case elements.



**Default Fonts** contains a list of case elements that you can associate with a font. Double clicking on a listed element opens the Font dialog so you can choose and associate a font with the listed case element. The font can be defined in terms of:

- Font
- Font style
- Size
- Script

The script attribute enables you to select the character set used.

## EnScript Tab

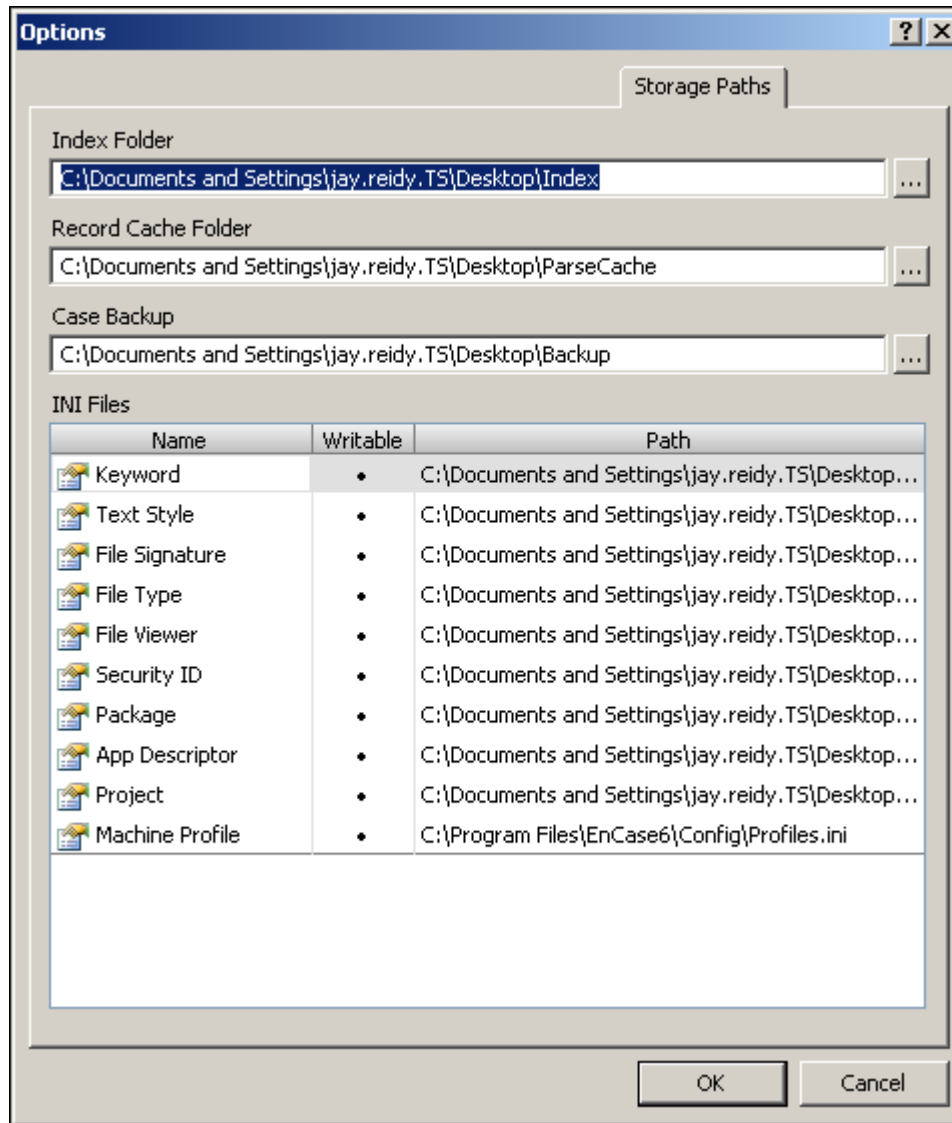
This tab enables you to specify the location of the include files library used by EnScript® programs.



**Include Path** displays the path and name of the folder that contains the include files library.

## Storage Paths Tab

The storage paths tab captures paths used for several files used by the EnCase® application.



The picture shows storage path default settings. You can change the index, cache, and backup folders by entering a new path or by navigating to and selecting the desired folder.

In the .ini files box, you can change an .ini folder's location and select whether it is writable.

## Sharing Configuration Files

Customization can be shared among investigators assigned to an investigation. Each of these INI files is populated by customizations the investigator makes while searching for evidence. The keyword and file signature files may be of particular interest. These case elements are distributed by sharing .INI files.

The application must be installed on the recipient machines.

*To share startup files:*

1. Click **Tools > Options > Storage Path**.

The Storage Path tab of the Options dialog displays.

2. Double-click on the row containing the desired INI file.

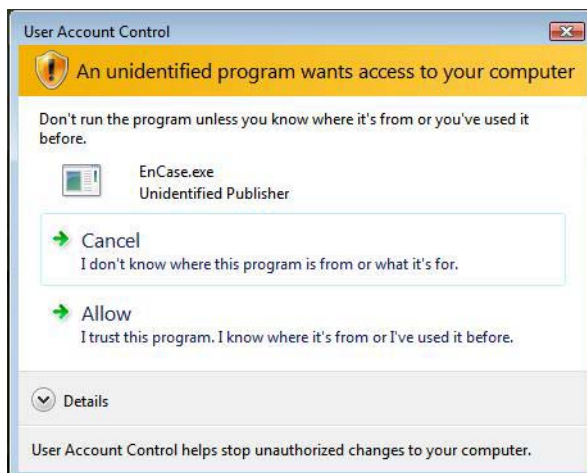
The Edit <.ini file name> dialog opens containing the path to the ini file.

3. To navigate to the .INI file, copy the path to the .INI file and paste it into Windows Explorer.
4. Copy the file and distribute it as desired.

## Vista Examiner Support

EnCase must run as an administrator in order to access the local Vista computer.

1. Start EnCase.
2. Vista displays a prompt with the heading **An unidentified program wants access to your computer:**



3. Click **Allow**.

Vista does not allow drag and drop between applications with different security levels. You must disable the User Account Control (UAC) to drag files to EnCase from the Windows shell. For details, see *Disabling Microsoft Windows Vista User Account Control* (on page 41).

## Disabling Microsoft Windows Vista User Account Control

You can use the User Account Control (UAC) security feature in Microsoft Windows Vista to perform common tasks as a non-administrator (called standard user) and as an administrator without having to switch users, log off, or use **Run As**.

In prior versions of Windows, the majority of user accounts were configured as members of the local administrator's group because administrator privileges are required to install, update, and run many software applications without conflicts and to perform typical system-level tasks.

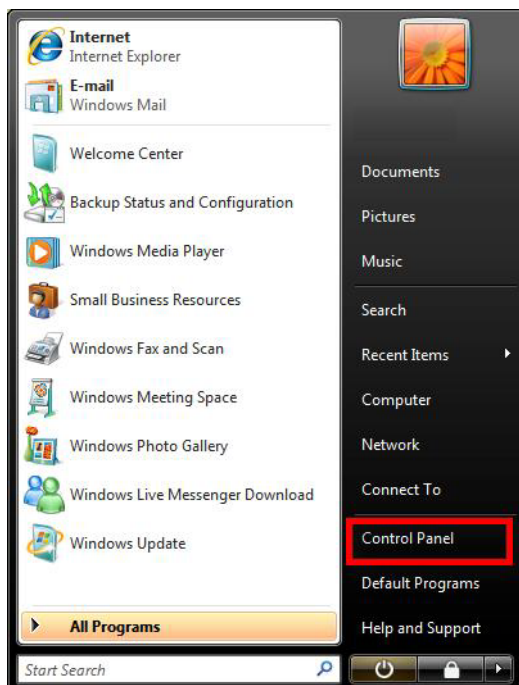
With UAC enabled, you can run most applications, components, and processes with a limited privilege, but have elevation potential for specific administrative tasks and application functions.

---

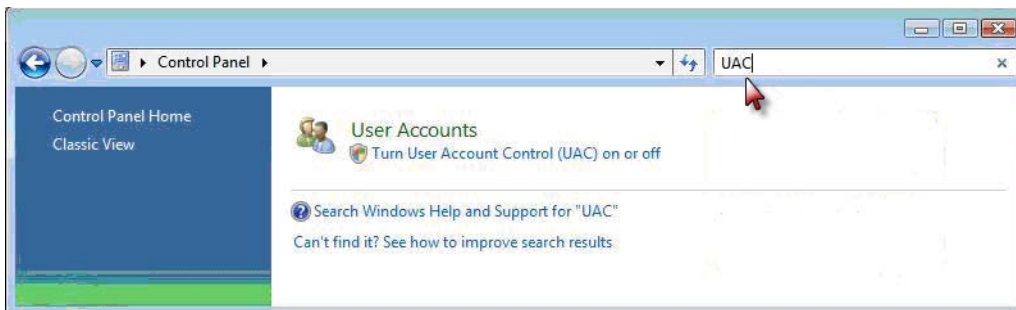
To disable UAC, you must be logged on with a credential that is a member of the local administrator group.

---

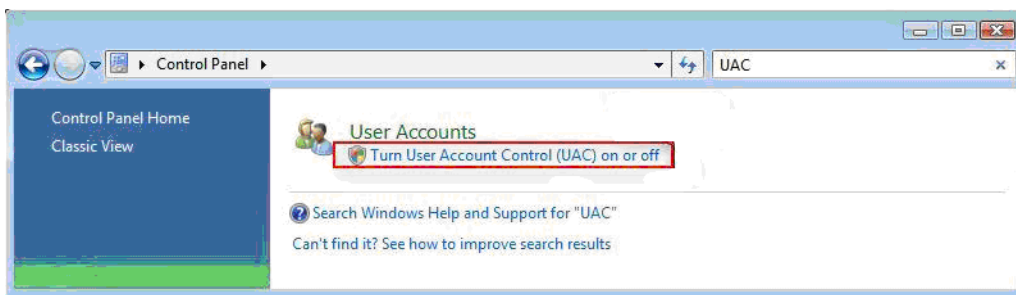
1. From the Start menu, select **Control Panel**.



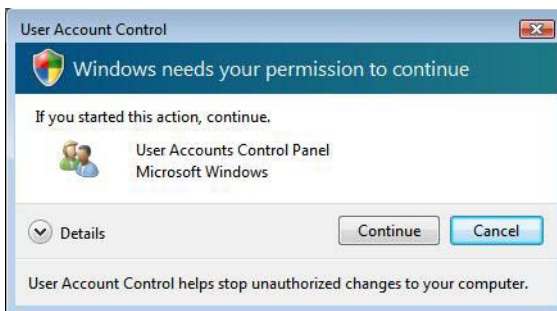
2. In the Control Panel Home window, enter **UAC** in the search field. The User Accounts option automatically displays under the search field.



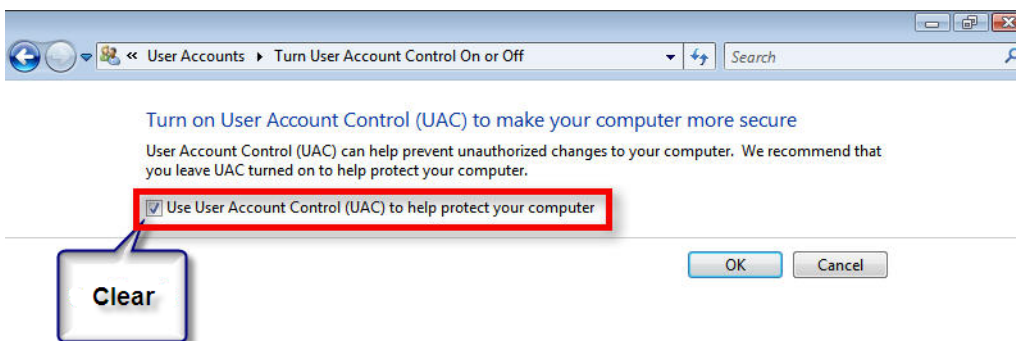
3. In the Control Panel Home window, select **Turn User Account Control (UAC) on or off**.



4. The User Account Control message displays, prompting you to continue or cancel.

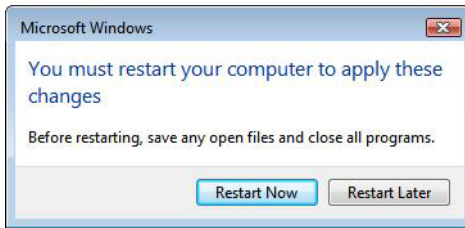


5. Click **Continue**.
6. In the Turn User Account Control On or Off window, clear the option for **Use User Account Control (UAC) to help protect your computer**, then click OK.





7. A message displays prompting you to restart your computer to apply these changes. Click **Restart Now** or **Restart Later** to close the User Accounts Task window.



## Running a 32-bit Application on a 64-bit Platform

There are limitations in running a 32-bit application (for example, EnCase, SAFE, or Servlet) on a 64-bit platform. You will only get basic snapshot information such as ports or processes. For full results, you must run the application on the correct platform.



# Using LinEn

- Introduction 45
- Viewing the License for LinEn 46
- Creating a LinEn Boot Disc 47
- Configuring Your Linux Distribution 48
- Performing Acquisitions with LinEn 50
- Hashing the Subject Drive Using LinEn 58

## Introduction

The LinEn™ utility runs on the Linux operating system and facilitates the following functions:

- Performing drive-to-drive acquisitions
- Performing crossover acquisitions

LinEn runs independently of the Linux operating system thus improving acquisition speeds, and runs in 32-bit mode (rather than 16-bit mode). Because Linux provides greater device support, LinEn can acquire data from a larger set of devices.

As with other operating systems, to prevent inadvertent disk writes, modifications to the operating system need to be made. Linux typically has a feature called **autofs** installed by default. This feature automatically mounts, and thus writes to, any medium attached to the computer. Instructions in this chapter describe how to disable this feature to protect the integrity of your evidence.

## Viewing the License for LinEn

LinEn must be running, and you must be on the LinEn main screen.

*To view the license for LinEn:*

1. Press **L**.  
The license displays.
2. Press **Enter**.  
The LinEn main screen displays.

## Creating a LinEn Boot Disc

If you want to run LinEn on the subject machine, you need to create a LinEn boot disc. When you create a LinEn boot disc, it is important to choose a "Live" Linux distribution, as these types of distributions are designed to run straight from the CD or DVD and do not install themselves on the subject machine.

You must have an ISO image of the live Linux distribution you want to use, such as Knoppix. Knoppix is one of the popular live distributions.

---

Note: As it is not practical to modify the settings of a live Linux distribution, ensure that the live distribution does not automatically mount detected devices.

---

To create a LinEn Boot disc

1. Using your EnCase application on the investigator's machine, click **Tools > Create Boot Disc**.

The Choose Destination page of the Create Boot Disk wizard displays.

2. Click **ISO Image**, and click **Next**.

The Formatting Options page of the Create Boot Disk wizard displays.

3. Provide a path and filename to the ISO image you downloaded earlier, optionally click **Alter Boot Table**, and click **Next**.

The Copy Files page of the Create Book Disk wizard displays.

4. Right-click in the right pane of the Copy Files page, and click **New**.

The file browser opens.

5. Enter or select the path to the LinEn executable, normally `c:\program files\encase6\linen`, click **OK**, then click **Finish**.

The Creating ISO progress bar displays on the Copy Files page. Once the modified ISO file is created, the wizard closes.

6. Burn the ISO file onto a blank CD/DVD using the burning software of your choice. For help with this, refer to the instructions that came with your software.

You now have a boot disc to run Linux and LinEn while you acquire the subject Linux device.

## Configuring Your Linux Distribution

Before LinEn can run on Linux, you must configure Linux distribution. Due to the nature of Linux and its distributions, only the following standard distributions are discussed:

- SUSE 9.1
- Red Hat
- Knoppix

---

Note: Because of the dynamic nature of Linux distributions, It is recommended that you validate your Linux environment before using it in the field.

---

The process describes an ideal setup process that effectively runs the LinEn application in a forensically sound manner.

Many distributions provide **autofs** as the means auto-mounting anything attached to the Linux system. It is essential that **autofs** is disabled to prevent auto-mounting.

## Obtaining a Linux Distribution

A Linux distribution can be obtained from any Linux vendor.

If you intend to use a LinEn boot disc, you will need a live distribution, such as Knoppix, in order to create a boot disc. If you intend to run LinEn on a installed version of Linux on your forensic machine, we recommend using SUSE or Red Hat.

For the Linux distributions discussed in relation to LinEn, obtain a distribution from one of the following:

- For the latest SUSE distribution, go to the [\*http://www.novell.com/linux/\*](http://www.novell.com/linux/) (<http://www.novell.com/linux/>) website.
- For the latest Red Hat distribution, go to the [\*http://www.redhat.com/\*](http://www.redhat.com/) (<http://www.redhat.com/>) website.
- For the latest Knoppix distribution, go to the [\*http://knoppix.com/\*](http://knoppix.com/) (<http://knoppix.com/>) website.

## LinEn Set Up Under SUSE

You must already have SUSE installed on your Linux machine.

1. Copy the LinEn executable from `C:\Program Files\EnCase6` on your Windows machine to the desired directory, `/usr/local/encase` on your Linux machine.
2. Open a command shell on your Linux machine.
3. Enter `chmod 777/usr/local/encase/linen`. This changes the permissions on the LinEn executable, so that it can be executed by everyone.
4. Close the command shell.
5. Click **Main Menu > System > Configuration > YaST**. Yet Another Setup Tool (YaST) is used to configure various settings for your Linux operating system.
6. Open the Runlevel Editor.
7. Ensure that **autofs** is disabled

## LinEn Set Up Under Red Hat

You must have Red Hat installed on your Linux machine.

1. Copy the LinEn executable from `C:\Program Files\EnCase6` on your Windows machine to the desired directory, `/usr/local/encase` on your Linux machine.
2. Open a command shell on your Linux machine.
3. Enter `chmod 777/usr/local/encase/linen`. This changes the permissions on the LinEn executable, so that it can be executed by anyone.
4. Close the command shell.
5. Click **Main Menu > System Settings > Server Settings**.
6. Ensure that the **autofs** is disabled.

## Performing Acquisitions with LinEn

The EnCase LinEn utility provides the following methods of acquiring evidence from a subject drive:

- Drive-to-drive acquisitions
- Crossover cable acquisitions

Drive-to-drive acquisitions provide the means to safely preview and acquire devices without using a hardware write blocker. Drive-to-drive acquisitions use either the subject machine or the forensic machine to perform the acquisitions. The Drive-to-drive acquisition speed can be significantly faster than EN.EXE and MS- DOS from previous versions, simply because Linux is a 32-bit operating system.

Crossover cable acquisitions require both a subject and forensic machine. This type of acquisition also negates the need for a hardware write blocker; however, it lends itself to situations where access to the subject machine's drive are difficult or not practical. This is the recommended method for acquiring laptops and exotic RAID arrays. This method is slower than a Drive-to-drive acquisition because data is transferred over a network cable, and thus is especially sensitive to the speed of the network cards housed in both machines.

### Setup for a Drive-to-Drive Acquisition

When a subject drive from the subject machine cannot be acquired via a crossover cable acquisition, the subject drive can be acquired via a drive-to-drive acquisition. Drive-to-drive acquisitions can be done in the following ways:

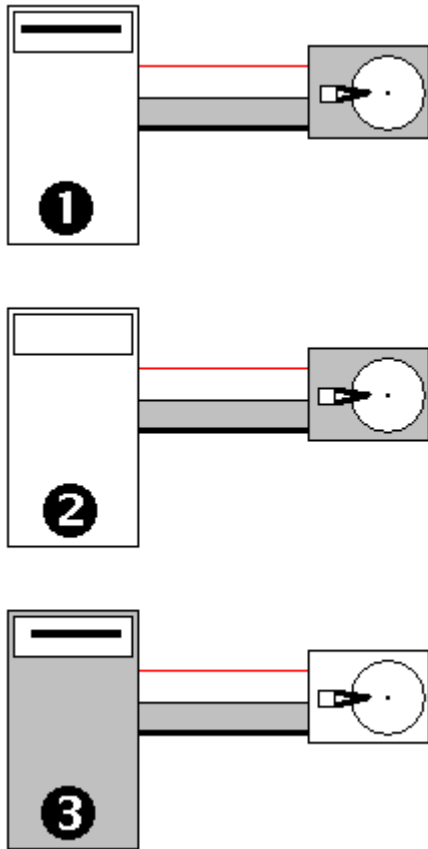
- Running a LinEn boot disc on the forensic machine
- Running the LinEn utility from Linux already installed on the forensic machine
- Running a LinEn boot disc on the subject machine

Any of these cables can be used as a hard disk cable:

- IDE Cable
- USB Cable
- Firewire
- SATA
- SCSI



Figure 3 Setups for Drive-to-drive acquisitions with 1) the forensic machine, running LinEn from the LinEn Boot Disk, connected to the subject hard drive; 2) the forensic machine, booted to Linux and running LinEn, connected to the subject hard drive; 3) subject machine, running LinEn from the LinEn Boot Disk, connected to the target hard drive.



## Doing a Drive-to-Drive Acquisition Using LinEn

Once LinEn is set up, run LinEn, choose **Acquire**, then select the drive to be acquired and the storage path. Optionally, provide additional metadata.

Configure LinEn as described in LinEn Setup, and verify that **autofs** is disabled (unchecked).

The investigator has identified the subject drive to be acquired and the storage drive that will hold the acquired evidence file.

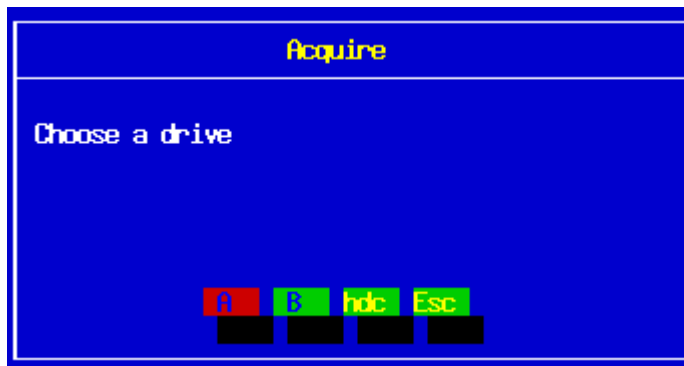
1. If the FAT32 storage partition to be acquired has not been mounted, mount the FAT32 storage partition.
2. Navigate to the folder where LinEn resides and type `./linen` in the console to run LinEn.

The LinEn Main Screen displays.

EnCase (6.0) (Linux)							
Code	Type	Sectors	Size	LP	Label	System	Size
Disk0 /dev/hda Linux 78165360 Sectors Size 37.3GB							
00	82	Linux Swap	1020096	498.1MB			
00	83	Linux EXT2	20972448	10.0GB			
00	83	Linux EXT2	9766512	4.7GB			
00	0C	FAT32X	46406304	22.1GB			
Disk5 /dev/hdd Linux 234375120 Sectors Size 111.8GB							
00	0C	FAT32X	40965750	19.5GB			
00	0C	FAT32X	61432560	29.3GB			
00	0C	FAT32X	65529135	31.2GB			
Disk9 /dev/sda Linux 64000 Sectors Size 31.2MB							
80	04	FAT16	64448	31.5MB			
				hda1	/dev/hda1	Linux	498.1MB
				hda2	/dev/hda2	Linux	10.0GB
				hda3	/dev/hda3	Linux	4.7GB
				hda4	/dev/hda4	Linux	22.1GB
				hdd1	/dev/hdd1	Linux	19.5GB
				hdd2	/dev/hdd2	Linux	29.3GB
				hdd3	/dev/hdd3	Linux	31.2GB
				sda1	/dev/sda1	Linux	31.4MB
Acquire ash Ser er uit							

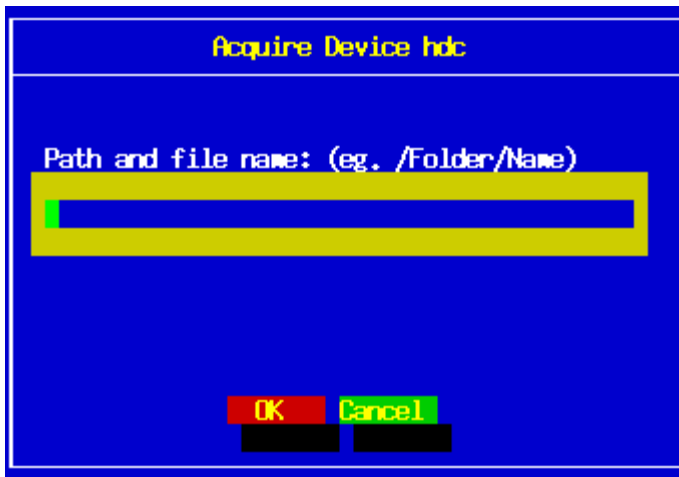
3. Select **Acquire**.

The Acquire screen displays.



4. Choose the physical drive or logical partition you wish to acquire.

The Acquire Device <drive> dialog displays.



5. For the data elements requested by the Acquire dialog, either accept the default, or enter a value or choose one of the alternatives, as described in Specifying and Running an Acquisition.

6. Press **Enter**.

The Acquire Device dialog requests additional data values until all data elements have been entered or selected. Then, the Creating File dialog displays.

7. When the acquisition is complete, click **OK**.

The LinEn main window displays. The subject has been acquired and is stored on the storage drive.

8. Connect the storage drive to investigator's machine.
9. Add the EnCase evidence file using the Sessions Sources page of the Add Device Wizard, as described in Completing the Sessions Sources Page

## Acquiring Device Configuration Overlays (DCO) and Host Protected Areas (HPA)

EnCase applications can detect and image DCO and/or HPA areas on any ATA-6 or higher-level disk drive. These areas are detected using LinEn (Linux) or the FastBloc SE module. EnCase applications running in Windows with a hardware write blocker will not detect DCOs or HPAs.

The application now shows if a DCO area exists in addition to the HPA area on a target drive. FastBloc SE is a separately purchased component.

HPA is a special area located at the end of a disk. It is usually configured so the casual observer cannot see it, and can only be accessed by reconfiguring the disk. HPA and DCO are extremely similar; the difference is the SET\_MAX\_ADDRESS bit setting that allows recovery of a removed HPA at reboot. When supported, EnCase applications see both areas if they coexist on a hard drive. For more information, see the EnCase Modules Manual.

## Acquiring a Disk Running in Direct ATA Mode

If the Linux distribution supports ATA mode, you will see a **Mode** option. The mode must be set before the disk is acquired. An ATA disk can be acquired via the drive-to-drive method. The ATA mode is useful for cases when the evidence drive has a host protected area (HPA) or drive control overlay (DCO). Only Direct ATA Mode can review and acquire these areas.

LinEn is configured as described in LinEn Setup, and **autofs** is disabled (unchecked). Linux is running in Direct ATA Mode.

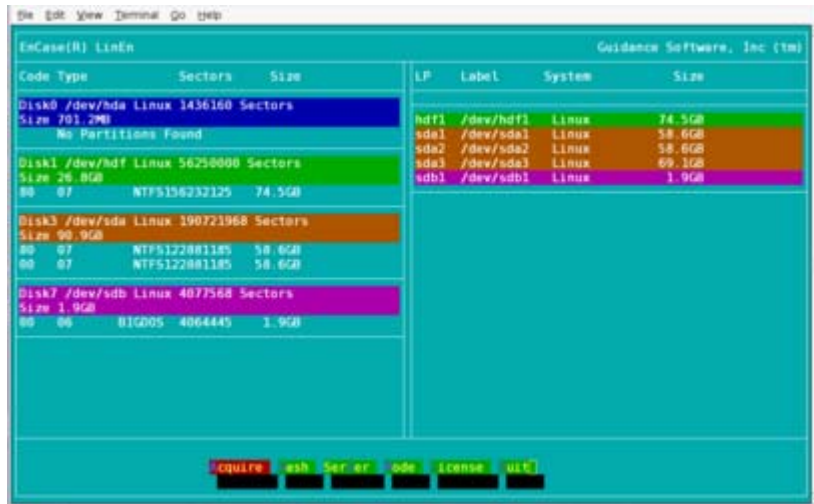
*To acquire a disk running in Direct ATA Mode:*

1. If the FAT32 storage partition to be acquired has not been mounted, mount the FAT32 storage partition.
2. Navigate to the folder where LinEn resides and type `./linen` in the console.  
The LinEn Main Screen displays.
3. Select **Mode**, then select Direct ATA Mode.  
The disk running in ATA mode can now be acquired.
4. Continue the drive-to-drive acquisition with Step 3 of Doing a Drive-toDrive Acquisition Using LinEn.

## Mode Selection

LinEn starts up in BIOS mode. A disk acquired in this mode reports only disk size seen by the BIOS. As a result, no data contained in a DCO are seen or reported. The **Mode** selection in LinEn provides a solution.

Notice Disk1 in the figure. It shows a disk size of 26.8 GB. If this is acquired now, only that quantity of data is identified.



The Linux distribution in use must support Direct ATA mode for this function to work.

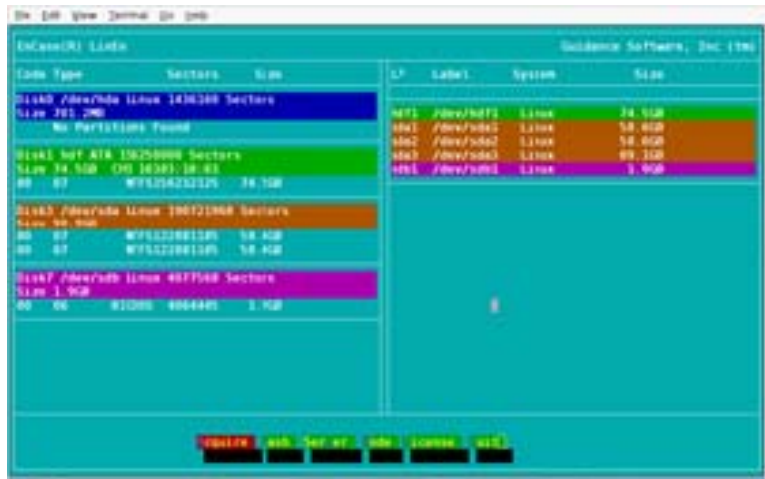
*To test for the presence of a DCO,*

1. Start LinEn in the normal manner on a computer that supports Direct ATA. The main screen shows a **Mode** button.



2. Enter 'M' to select Mode. A second screen displays offering three acquisition selections:
  - BIOS
  - ATA
  - Cancel
3. Enter 'A' to select ATA Mode.

If a DCO is present on the disk, the original LinEn screen reports the correct disk size and the correct number of sectors. Disk1 in the following illustration shows the true disk size, 75.5 GB.



Acquire the disk according to protocol.

## Doing a Crossover Cable Preview or Acquisition

You have a LinEn boot disk.

The investigator has identified the subject drive to be acquired.

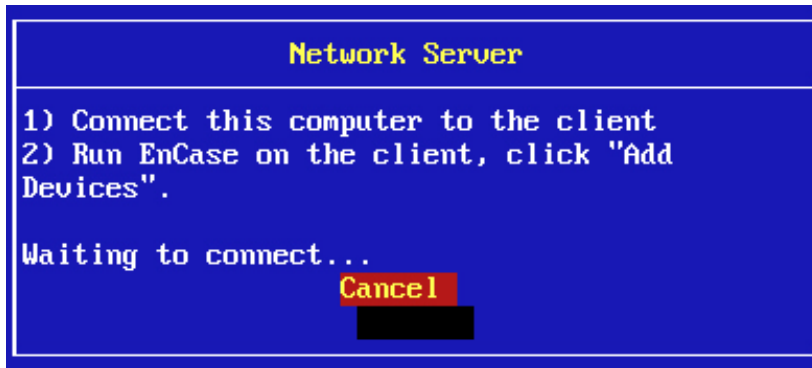
### *To do a crossover cable acquisition*

1. Boot the subject machine from the LinEn boot disk.
2. Connect the forensic machine to the subject machine using a crossover cable.
3. In Linux, ensure that the subject machine has an IP address assigned and a NIC card loaded appropriately by typing `ifconfig eth0`, then if no IP address is assigned, assign one by typing `ifconfig eth0 10.0.0.1 netmask 255.0.0.0`, and check the IP address assignment again by typing `ifconfig eth0`.
4. Navigate to the folder where LinEn resides and type `./linen` in the console to run LinEn.

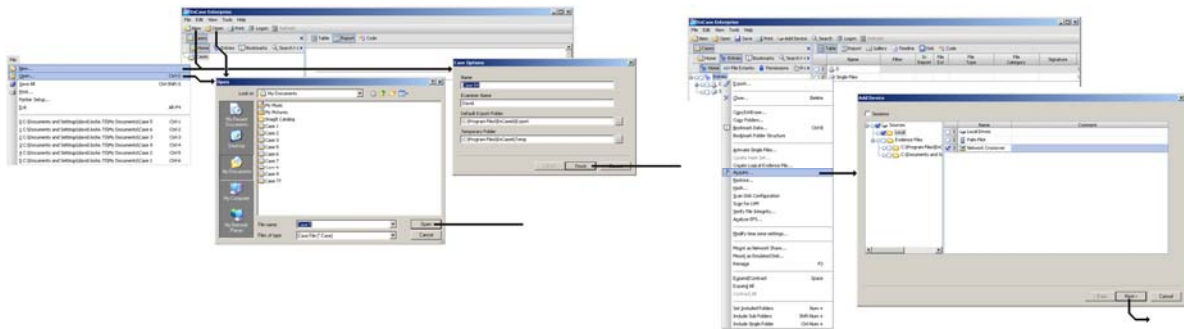
The LinEn Main Screen displays.

5. Select **Server**, and press **Enter**.

The message Waiting to connect should display.



6. Specify an IP address of 10.0.0.1 on the forensic machine for the subject machine.
7. Launch the EnCase application on the forensic machine.



8. Create a new case, or open an existing case.
9. Right-click on the **Devices** object, and click **Add Device**.
10. Select **Network Crossover**, and click **Next**.
11. Select the physical disk or logical partition to acquire or preview and click **Next**.
12. Click **Finish**.

The contents of the selected device reached through the network crossover connection are previewed. To acquire the content, perform an acquisition as described in Specifying and Running an Acquisition

## Hashing the Subject Drive Using LinEn

This allows the investigator to know the hash value of the drive.

LinEn is configured as described in the setup topics, and **autofs** is disabled.

The investigator has identified the subject drive to be hashed.

### *To perform a hash using LinEn*

1. Navigate to the folder where LinEn resides and type `./linen` in the console.  
The LinEn Main Screen displays.
2. Select **Hash**.  
The Hash dialog displays.
3. Select a drive, and click **OK**.  
The Start Sector dialog displays.
4. Accept the default or enter the desired **Start Sector**, and click **OK**.  
The Stop Sector dialog displays.
5. Accept the default or enter the desired **Stop Sector**, and click **OK**.  
The (Hash Results) dialog displays.
6. If you want the hash result to be written to a file, click **Yes**.  
If you are saving the hash value to a file, the Save Hash Value to a File dialog displays; otherwise, the LinEn Main Screen displays.
7. Enter the path and filename of the file that will contain the hash value, and click **OK**.  
The hash value is saved, and the LinEn Main Screen displays.

A hash value is calculated for the selected sectors of the selected file. You can save this hash value to a file.



# Navigating the EnCase Interface

■	The Main Window	60
■	Panes and their Specific Tabs	98
■	Navigating the Tree Pane	115
■	Modifying the Table Pane	122
■	Modifying the View Pane	148

## The Main Window

Begin using the EnCase application in the main window.

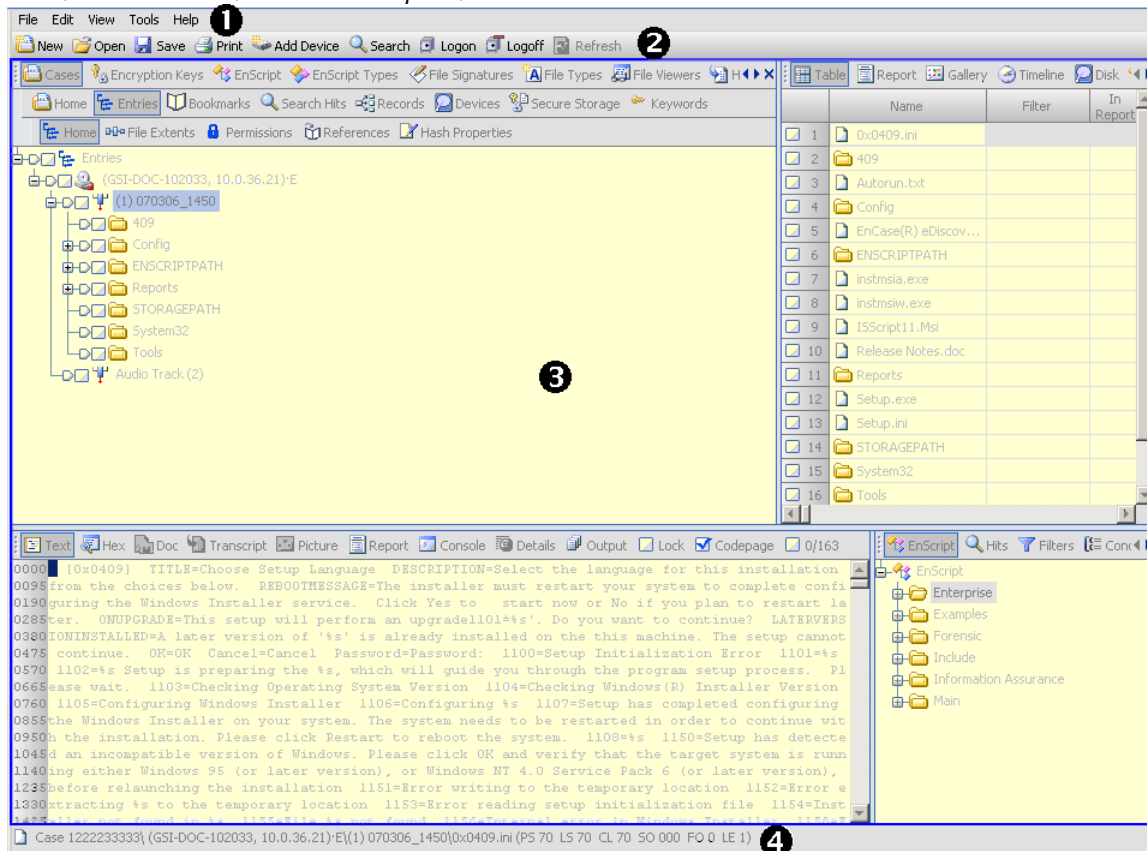
The main window organizes the application's features. Features accessible from the main window are run from the system menu, the toolbar, and various right-click menus. As the application runs, a status message displays in the status line at the bottom of the window.

The main window consists of a

- System menu
- Toolbar
- Window containing panes
- Status line

Panes divide and organize the window and contain trees, tables, and data in various representations.

*Figure 4 The Main Window as it appears in EnCase Enterprise with an open case, 1) indicates the system menu, 2) the toolbar, 3) a window pane, and 4) the status line.*

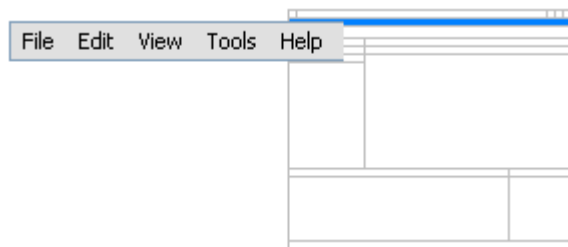


The menus, commands, and icons displayed in the toolbar change depending on the context configuration of the application. The Logon and Logoff icons, for example, appear in enterprise-capable applications only. The Edit menu does not appear when the application is opened in acquisition only mode, which occurs when the application is opened on a machine that does not have a dongle or appropriate licenses. Additional functionality modules add commands and icons.

## System Menu

The system menu organizes commands provided by the EnCase application.

The system menu appears in the main window. The system menu, along with the right-click, context-specific menus, provides commands to execute application functionality.



The system menu contains the following commands:

- File
- Edit
- View
- Tools
- Help

When clicked, the commands in the system menu display the corresponding menu. The Edit menu does not display in acquisition mode, although the Edit command always displays in the system menu.

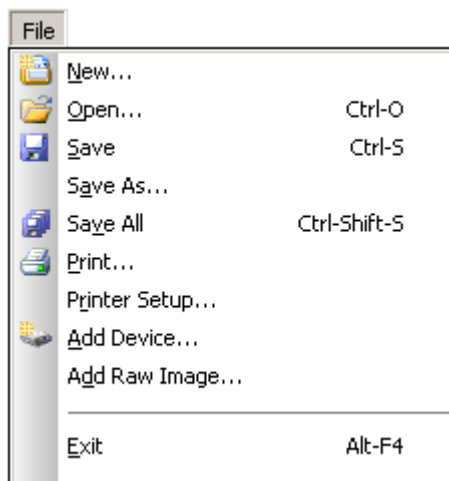
Some of the commands in the menus displayed by the system menu commands are context dependent. Context-dependent commands appear in the menus, but are disabled unless the current application context makes them available.

## File Menu

The File menu provides commands that manipulate application files and global application settings.

You can

- create new case files
- open existing case files
- save case files and global settings
- print the contents of files
- add devices to cases
- add raw images to cases
- exit the application



You may see different options on the File menu, depending on your context.

The File menu provides the following commands:

**New** displays the Case Options dialog where you define the case you want to add.

**Open** displays the Open dialog where you select a previously saved case.

**Save** saves the previously saved case file, or displays the Save dialog where you enter the filename, path, and file type for the case file you want to save.

**Save As** displays the Save As dialog where you enter the filename, path, and file type for the case file under a different name.

**Save All** displays the Save All dialog where you enter the filename, path, and file type for both the case file and EnCase global settings.

**Print** displays a Print dialog, where you define the print settings for the content (Table, Report, Code), depending on what is displayed in the Table pane.

**Printer Setup** displays the Print Setup dialog where you select a printer and choose printer settings.

**Add Device** displays the Add Device wizard where you define the preview and acquire parameters for a device. This command appears in the menu only when a case is open.

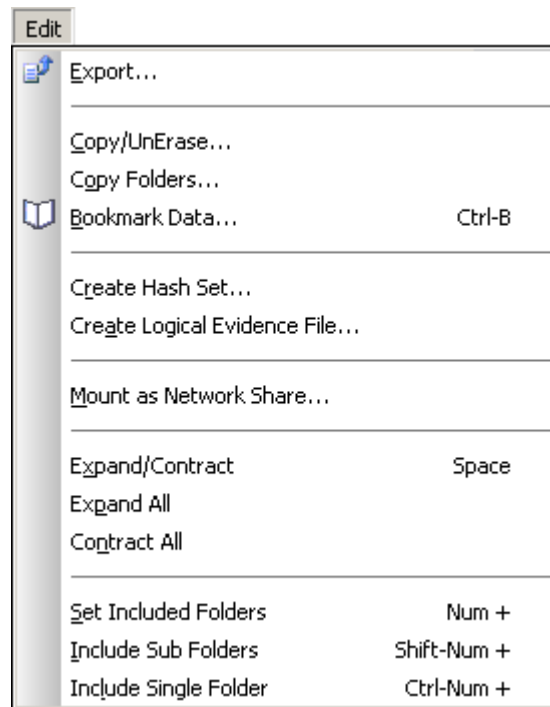
**Add Raw Image** displays the Add Raw Image dialog where you select image files to be added to the open case. This command appears in the menu only when a case is open.

**Exit** closes the program. If content has changed, you are prompted to save it.

## Edit Menu

The Edit menu commands work with the objects and content in the currently selected tab.

Edit menu commands are context-specific, changing as you move from one tab to another, or select objects or content in a tab. Specific Edit menus are discussed in sections describing the features that have an Edit menu associated with them.



The Edit menu shown here provides the following commands:

**Export** displays the Export dialog, where you select fields in a file to copy data to a text file, and specify the path for the file containing the data.

**Copy/UnErase** starts the Copy/UnErase wizard for copying evidence files and folder entries to one or more destination files. This command does not change the evidence file.

**Copy Folders** displays the Copy Folders dialog, where you can process the content of a selected folder or folders in a variety of ways.

**Bookmark Data** displays the Bookmark Data dialog, where you can create and define a new data bookmark.

**Create a Hash Set** displays the Create Hash Set dialog for selected files already hashed. You can name and categorize the hash set to be created.

**Create Logical Evidence File** displays, for a selected file or collection of selected files, the Create Logical Evidence wizard, so you can create a new logical evidence file to contain those files.

**Mount as Network Share** displays the Mount as Network Share dialog, so you can mount an acquired device as a network share. This command appears only if the Virtual File System module is installed.

**Expand/Contract**, for a selected object anywhere along the branch of the tree, expands the branch of the tree, or for a fully expanded branch of the tree, contracts the branch.

**Expand All** expands all branches of the tree.

**Contract All** contracts all branches of the tree.

**Set Included Folders** is a toggle switch. It initially sets **Select All** for the selected object in a tree and its branches. Choosing it again clears the selected nodes.

**Include Sub Folders** toggles **Select All** for the selected object in a tree and its branches.

**Include Single Folder** toggles **Select All** for the selected object in a tree, ignoring its branches.

## Copy/UnErase

The Copy/UnErase command recovers and unerases files with byte-per-byte precision.

*To initiate Copy/UnErase:*

1. Click **Edit > Copy/UnErase**.
2. Select the file or files to copy.
3. Select whether to have each recovered file appear in a new file or to merge them to a single file.

4. Enter a replacement character for erased FAT table entries. The default is an underscore.
5. Click **Next**.
6. To determine what is to be Copy/UnErased, do one of the following:
  - a. If only the logical files are to be Copy/UnErased, click **Logical Files Only**.
  - b. If the entire physical file is to be Copy/UnErased, click **Entire Physical File**.
  - c. If RAM and Disk slack are to be Copy/UnErased, click **RAM and Disk Slack**.
  - d. If only RAM slack is to be Copy/UnErased, click **RAM Slack Only**.
7. To determine which mask will be applied to the filenames of Copy/UnErased content, do one of the following:
  - a. For no masking, click **None**.
  - b. If non-ASCII characters are to be masked, click **Do not write non-ASCII character**.
  - c. If a dot is to be substituted for non-ASCII characters, click **Replace non-ASCII characters with DOT**.
8. If errors are to be included, click **Select Show Errors**, and then click **Next**.
9. If a destination folder other than /Export is to be used, select a destination folder.
10. Click **Finish**.

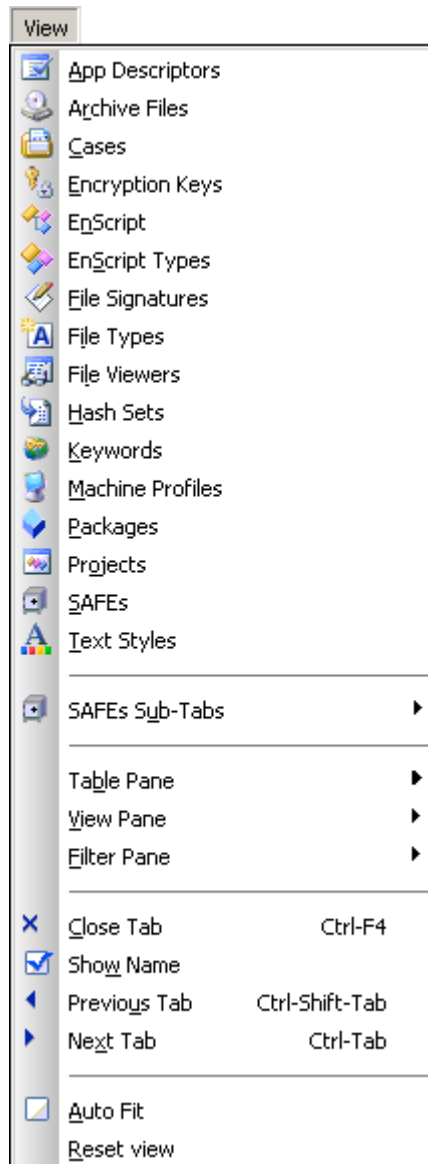
## View Menu

The View menu provides commands that determine the contents of the EnCase window panes.

View menu commands:

- Display specific tabs in the tree pane
- Display tabs that otherwise are not displayed, or that otherwise do not appear in the tree pane
- Toggle controls that appear in tab bars and the wrapping of the tool bar
- Navigate between tabs, hide tabs, and control the display of tabs with or without their names
- Move any tab containing windows back to their usual position in the main window





**App Descriptors** displays the App Descriptor tabs in the tree pane, which includes the App Descriptor-Home and App Descriptors- Hash Properties tabs. By default, these tabs are not displayed.

**Archive Files** displays the Archive File tab in the tree pane . This tab does not display by default.

**Cases** displays the Cases tabs in the tree pane, which includes the Cases-Home, Cases-Entries, Cases-Bookmarks, Cases-Search Hits, Cases-Records, Cases-Devices, Cases-Secure Storage, and Cases-Keywords tabs. These tabs display by default. Use this command if you previously closed the Cases tab.

**Encryption Keys** displays the Encryption Keys tab in the tree pane. This tab displays by default. Use this command if you previously closed the Encryption Key tab.

**EnScript** displays the EnScript tab in the tree pane. This tab does not display by default. When this tab displays, the EnScript tab in the Filters pane is closed.

When the EnScript tab appears in the Filter pane, the EnScript programs are organized into a tree extending to the programs themselves.

When the EnScript tab appears in the Tree pane, only folders populate the tree, and the programs themselves appear in a table in the Table pane.

The table representation contains information beyond what is visible in the tree representation in the Filter pane.

**EnScript Types** displays the EnScript Types tab in the tree pane. It does not display by default.

**File Signatures** displays the File Signatures tab in the tree pane. It does not display by default.

**File Types** displays the File Types tab in the Tree pane. It does not display by default.

**File Viewers** displays the File Viewers tab in the tree pane. It does not display by default.

**Hash Sets** displays the Hash Set tabs in the tree pane, which includes the Hash Sets-Home and Hash Sets-Hash Items tabs. They do not display by default.

**Keywords** displays the Keywords tab in the tree pane. It does not display by default.

**Machine Profiles** displays the Machine Profiles tabs in the tree pane, which includes the Machine Profiles- Home and Machine Profiles-Allowed tabs. They do not display by default.

**Packages** displays the Packages tab in the tree pane. It does not display by default.

**Projects** displays the Projects tab in the tree pane. It does not display by default.

**SAFEs** displays the SAFEs tabs in the Tree pane, which includes:

- ☐ the SAFEs- Home
- ☐ SAFEs-Network
- ☐ SAFEs-Roles
- ☐ SAFEs-Users
- ☐ SAFEs-Events

They do not display by default.

**SAFEs or Cases Sub- Tabs** displays a sub-menu associated with the tab currently displayed (SAFEs or Cases). In the figure above, the **SAFEs Sub-Tabs** command displays because the SAFEs tab is displayed in the Tree view (not shown) If Cases were displayed, then the command would be **Cases Sub-Tabs**.

**Table Pane** displays the Table Pane menu.

**View Pane** displays the View Pane menu.

**Filter Pane** displays the Filter pane menu.

**Close Tab** hides the tab currently in use. Once hidden, a tab can only reappear if it is opened using the tab commands on the View menu.

**Show Name** toggles the display of the name of the tab currently in use.

**Previous Tab** selects the tab to the left of the tab currently in use. When the tab currently in use is the leftmost tab, the rightmost tab is selected.

**Next Tab** selects the tab to the right of the tab currently in use. When the tab currently in use is the rightmost tab, the leftmost tab is selected.

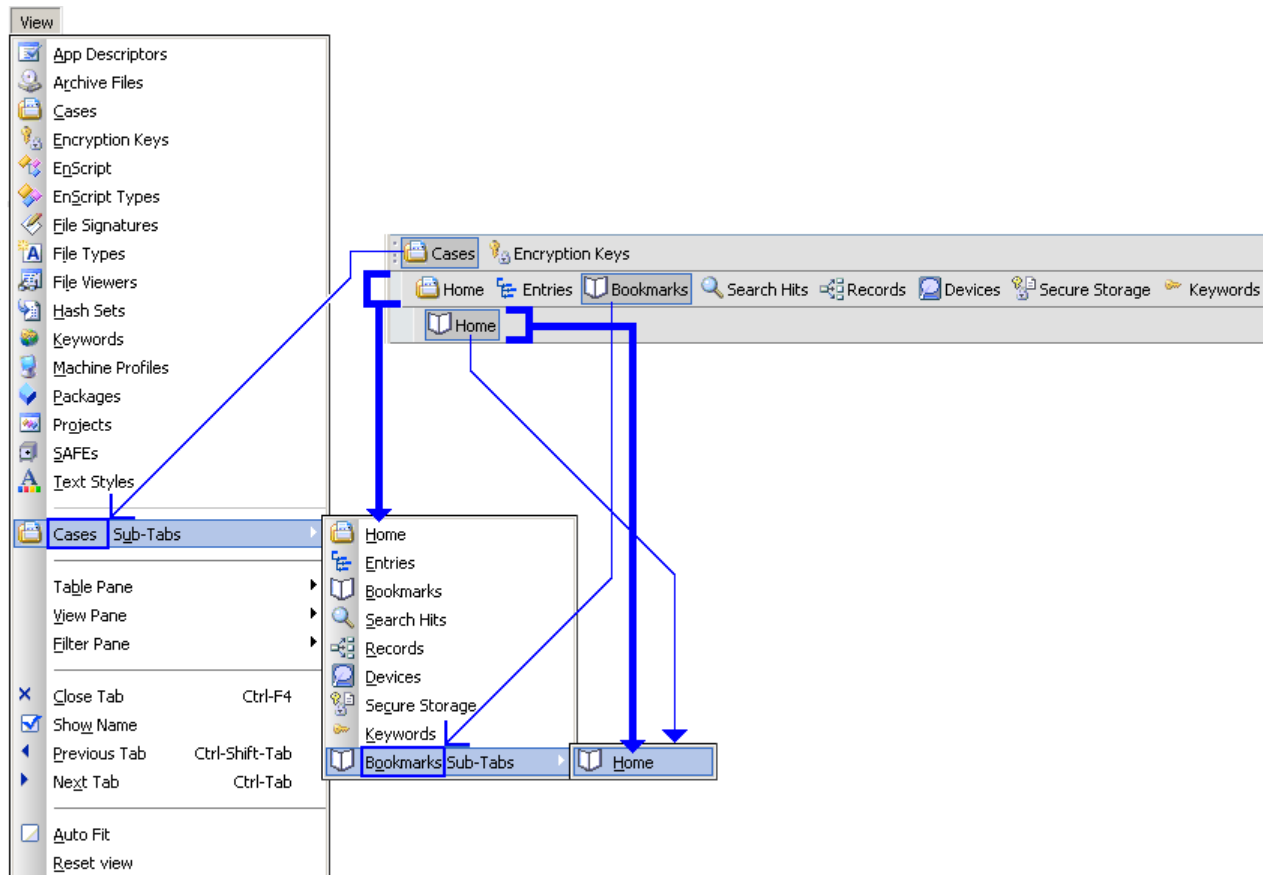
**Autofit** toggles the wrapping of the toolbar. The toolbar extends to the right beyond the tab when Autofit is not selected. When Autofit is selected, the toolbar wraps, so that the entire toolbar displays.

**Reset View** puts any tabs appearing in windows back into the main window in their usual locations.

## The Tree Pane and its Tab and Sub-Tab Menus

Sub-Tab menus display commands for tabs contained by parent tabs.

When a tab contains other tabs, it has a View command that displays a sub-tab menu. The sub-tab menu contains commands that display each of the contained tabs.



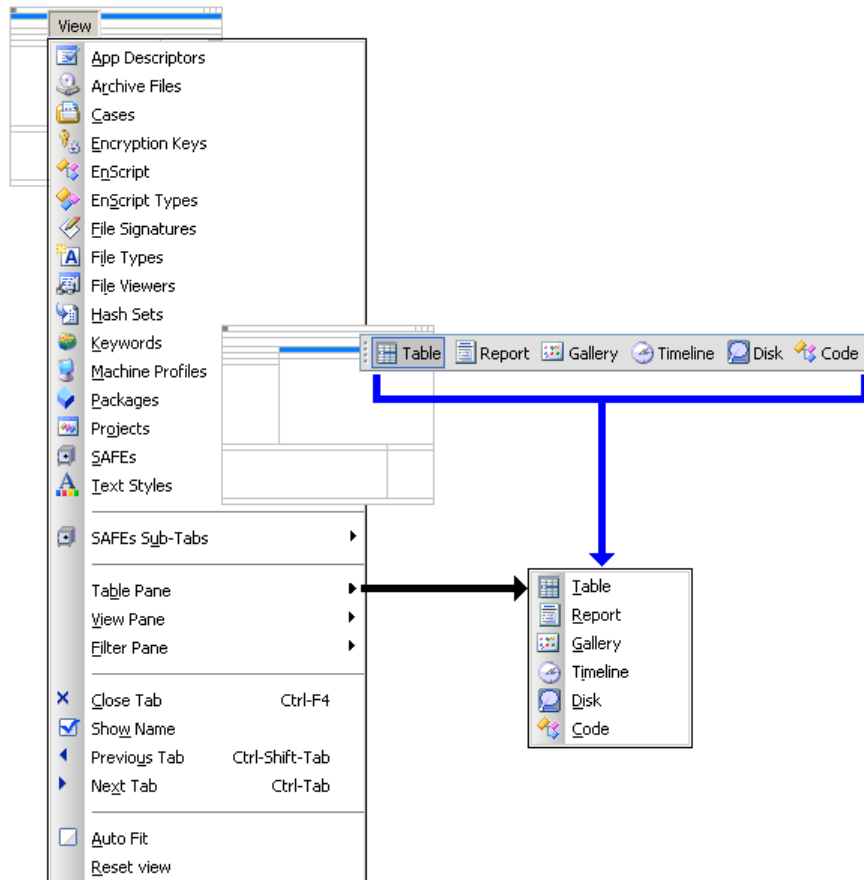
When a tab contains only one other tab, selecting the containing tab is equivalent to selecting the contained tab. For example, selecting **Cases Sub-Tabs > Bookmarks** is equivalent to selecting **Cases Sub-Tabs > Bookmarks Sub- Tabs > Home**.

The commands in the Sub-Tab menus open their corresponding tab or display a corresponding Sub-Tab menu.

## The Table Pane and its Tab Bar and View Menu

The Table Pane menu corresponds to the tabs appearing in the table pane.

The tabs in the table pane depend on the tab currently selected in the tree pane.

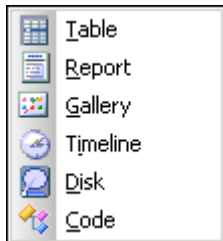


## Table Pane Menu

The **Table Pane** command on the View menu displays the Table Pane menu.

The table pane contains a collection of context-sensitive tabs. The context is driven by the tab displayed in the tree pane. The table pane menu is context-sensitive as well.

Each of the tabs in the Table pane has a corresponding tab in the Table pane tab bar, and a corresponding command on the Table Pane menu.



**Table** displays the Table tab in the table pane. It displays by default.

**Report** displays the Report tab in the table pane. It displays by default.

**Gallery** displays the Gallery tab in the table pane. It displays by default.

**Timeline** displays the Timeline tab in the table pane. It displays by default.

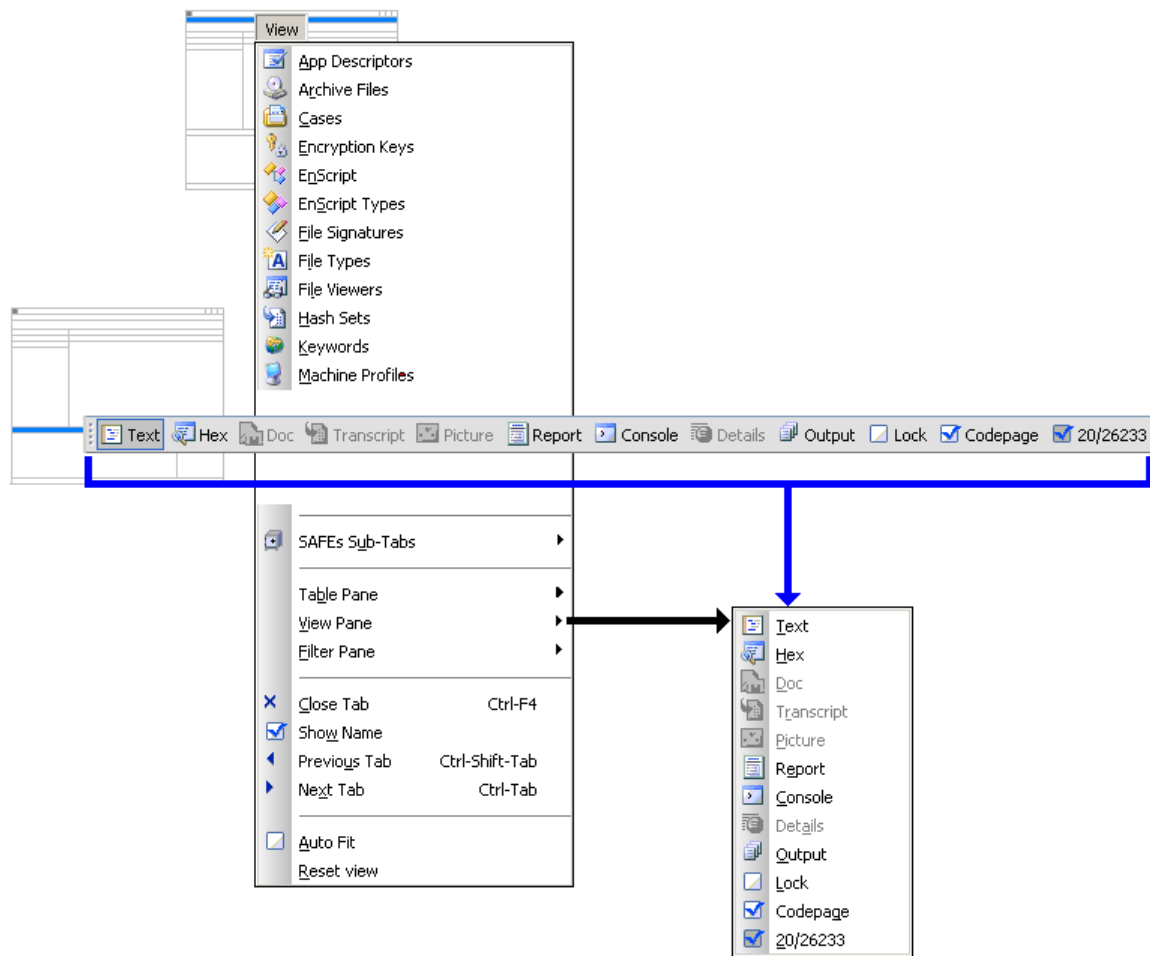
**Disk** displays the Disk tab in the table pane. It displays by default.

**Code** displays the Code tab in the table pane. It displays by default.

## The View Pane and its Tab Bar and View Menu

The View Pane menus display a command for each of the tabs on the table pane tab bar.

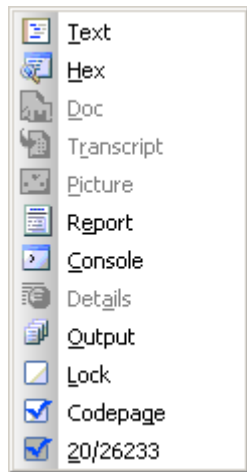
The View pane contains several tabs, depending on the tab currently selected in the table pane. The tab bar also includes controls that appear in the View pane menu.



## View Pane Menu

The **View Pane** command on the View menu displays the View Pane menu.

The View Pane menu contains commands corresponding to the tabs displayed in the View pane. Clicking one of these commands displays the corresponding tab in the View pane.



**Text** displays the ASCII text tab in the View pane.

**Hex** displays the Hexadecimal value tab in the View pane.

**Doc** displays a Windows document representation (if possible) in the View pane.

**Transcript** displays the Transcript tab in the View pane.

**Picture** displays the Picture tab in the View pane.

**Report** displays the Report tab in the View pane.

**Console** displays the Console tab in the View pane.

**Details** displays the Details tab in the View pane.

**Output** displays the Output tab in the View pane.

**Lock** prevents the View tab from changing the tab, based on the entry selected in the Table pane.

**Codepage** toggles the ability for the view pane to display the file information using the detected Code Page. If not selected, the default Code Page is used.

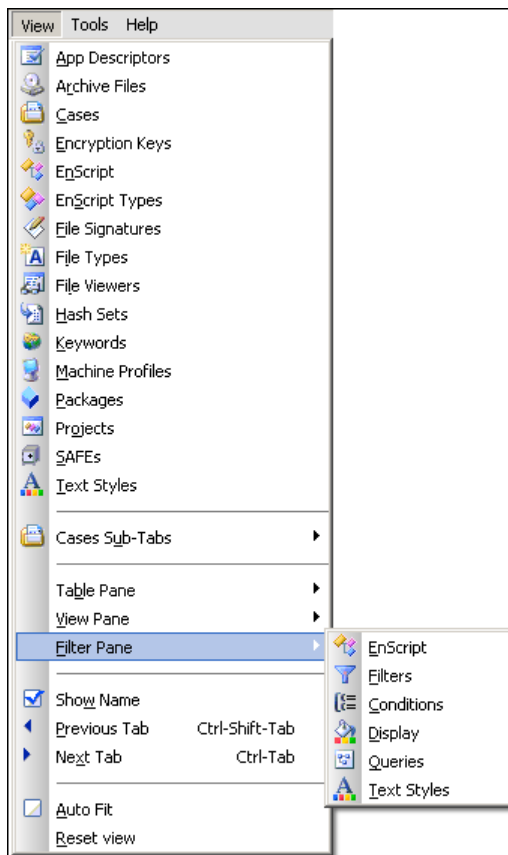
**Selection Indicator** indicates the number of selected items as well as the number of total possible items.



## The Filter Pane and its Tab Bar and View Menu

The Filter Pane menus display a command for each of the tabs that appear on the Filter pane tab bar.

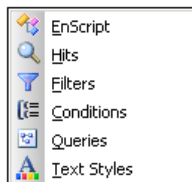
The Filter Pane menu and the tab bar for the Filter pane display commands corresponding to the tabs appearing in the View pane.



## Filter Pane Menu

The **Filter Pane** command on the View menu displays the Filter Pane menu.

The Filter Pane menu contains commands corresponding to the tabs displayed in the Filter pane. Clicking one of these commands displays the corresponding tab in the Filter pane.



**EnScript** displays the EnScript tab in the Filter pane.

**Filters** displays the Filters tab in the Filter pane.

**Conditions** displays the Conditions tab in the Filter pane.

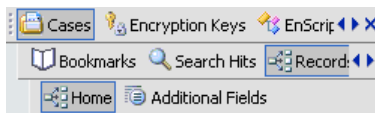
**Display** shows active filters.

**Queries** displays the Queries tab in the Filter pane.

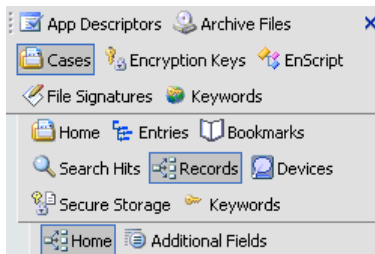
**Text Styles** displays the Text Styles tab in the Filter pane.

## Auto Fit

When you resize a window pane some tabs may not be viewable.



Instead of scrolling to them, you may want to use Auto Fit.

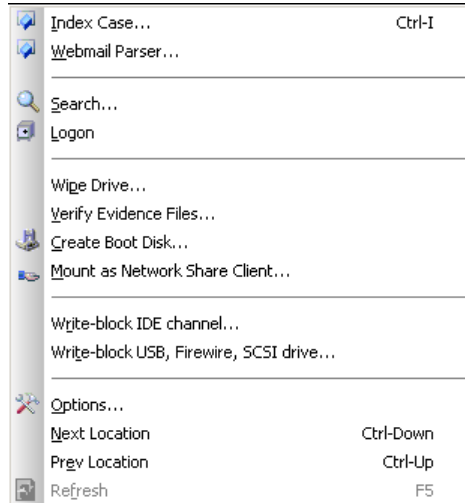


There are two ways to implement Auto Fit:

- Click **View > Auto Fit**.
- Right-click in the pane and select **Auto Fit**.

## Tools Menu

The Tools menu provides commands to perform analytical operations.



**Index Case** opens the Index Case dialog, where you include (or exclude) files in the indexing process. You can select a noise file, which is a list of stop words (words that will not be indexed).

**Webmail Parser** opens the Webmail Parser dialog, where you select the webmail vendors whose account files are to be parsed.

**Case Processor** starts the EnScript Case Processor script. You can also start it by opening the Forensic and Enterprise trees in the Filter pane and double-clicking. The shortcut hot key to start it is Alt+P.

**Sweep Enterprise** starts the EnScript Sweep Enterprise EnScript script. You can also start it by opening the Forensic and Enterprise trees in the Filter pane and double-clicking. The shortcut hot key is Alt+S.

**Search** opens the Search dialog, where you determine

- ☐ which files are searched
- ☐ define keyword searches
- ☐ perform email searches
- ☐ hash computing, and
- ☐ other search options

**Logon** opens the Logon wizard, where you can log on to the enterprise LAN.

**Logoff** logs you off the enterprise LAN.

**Wipe Drive** opens the Wipe Drive wizard, where you select media you want to completely erase. After using Wipe Drive, you must format the media.

**Verify Evidence Files** opens the Verify Evidence Files browser, where you select files to be verified. Verifying checks the Cyclical Redundancy Check (CRC) values to ensure evidence was not altered.

**Create Boot Disk** opens the Create Boot Disk wizard to create a LinEn boot disk.

**Mount as Network Share Client** opens the Mount as Network Share dialog, where you specify the IP address of the server to be mounted.

**Options** opens the Options dialog, where you define global settings for EnCase, such as

- ☐ default file locations for a new case
- ☐ fonts to use
- ☐ highlighting colors seen in the table pane
- ☐ date and time formats

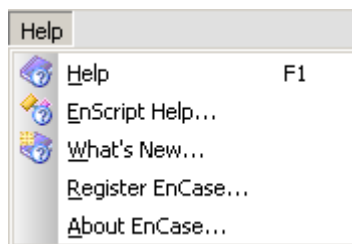
**Refresh** updates the EnCase views based on the content of the folder displayed in the lists or trees. Use this command when you use Windows to add files to the folders of an open case. EnCase is not aware of these changes until you refresh the lists and trees.

## Help Menu

The Help menu provides commands that access information and perform tasks associated with using your EnCase® application.

Using the Help menu you can

- display the readme help file
- register your application
- find out about your application
- get information about your license,
- learn what modules are installed, and other information.



**What's New** displays the EnCase Release Notes as a help file.

**Register EnCase** displays the application registration page, where you can

- Find your dongle serial number
- If connected to the Internet, register your application
- If not connected to the internet, find instructions on how to register your application

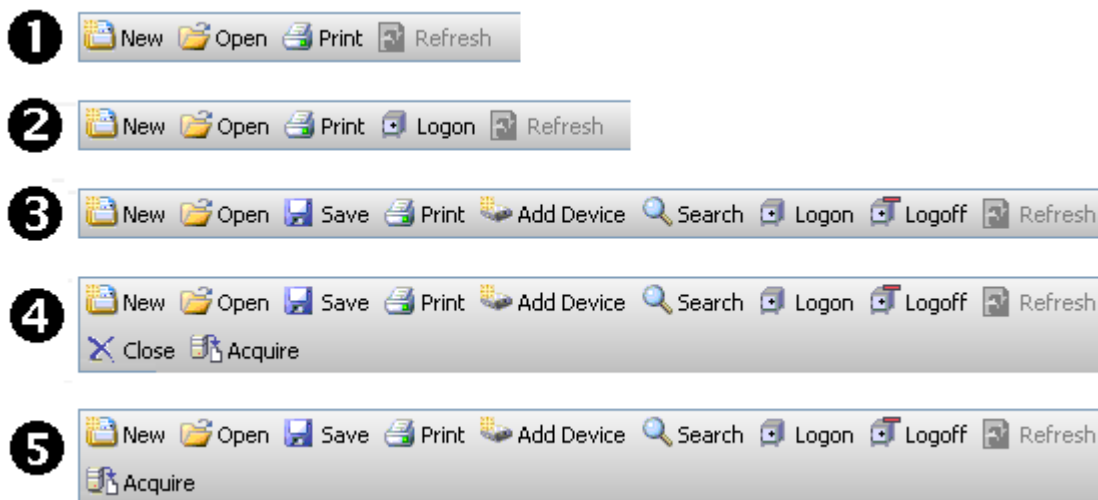
**About EnCase** tells you which version of EnCase, and which modules, you have installed.

## Toolbar

The toolbar provides icons for the most frequently used EnCase® program functionality.

The toolbar displays on the main window. It contains icons for performing the most frequent tasks in the current application mode or context. When EnCase® opens in acquisition mode, only the **New**, **Open**, **Print**, and **Refresh** icons appear in the toolbar. Once a case is opened, the **Add Device** icon appears. When the application is an enterprise application, the **Logon** icon appears, and once logged on, the **Logoff** icon displays.

*Figure 5 The Main Window Toolbar in Different Modes and Contexts, showing 1) Acquisition mode, and the rest in EnCase Enterprise 2) before logging in and opening a case, 3) after logging in and opening a case, 4) with an acquired device selected from the Entries tree, and 5) with an entry selected from the Entries table.*



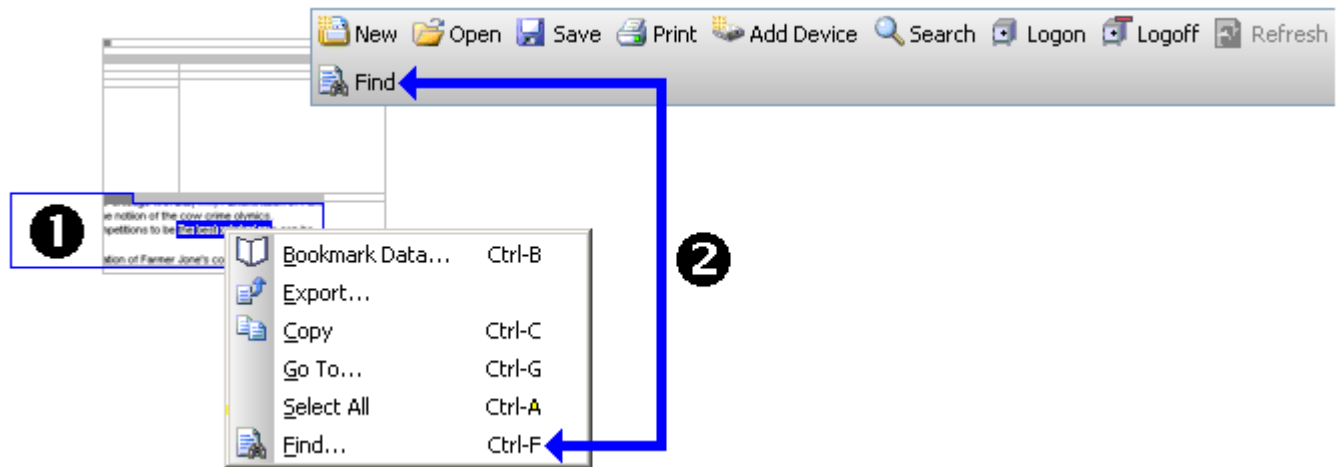
There is a corresponding menu command for each toolbar icon.

When the toolbar is wider than the main window, the toolbar wraps to another line.

Some icons are enabled only when they are useful, such as **Print** and **Refresh**.

The panes and the tabs in the toolbars also provide context- dependent icons for functionality, accessed through context- dependent, right-click menus provided in those features.

*Figure 6 A Context-dependent Icon and Its Associated Right-Click Menu Command, where 1) is the context for the right-click menu, and 2) is the corresponding menu command and toolbar icon. The Find command opens the Find dialog where a search string can be defined that searches within the content highlighted in the View pane.*



**New** displays the Case Options wizard where a new case is defined.

**Open** displays the Open dialog where you can open an existing case.

**Print** displays the Print dialog.

**Refresh** updates a list or table to reflect changes made in the file system to files that drive the EnCase application.

**Save** displays, once a case is opened, the Save dialog.

**Add Device** displays, once a case is opened, the Add Device wizard, so that a device can be previewed or acquired.

**Search** displays the Search dialog, so that evidence associated with the case can be searched.

**Logon** displays the Logon dialog, so that you can log on to the SAFE. This icon only appears in enterprise applications.

**Logoff** logs you off the SAFE. This icon only appears after you have logged on to the SAFE.

Other icons are described in the context where they appear.

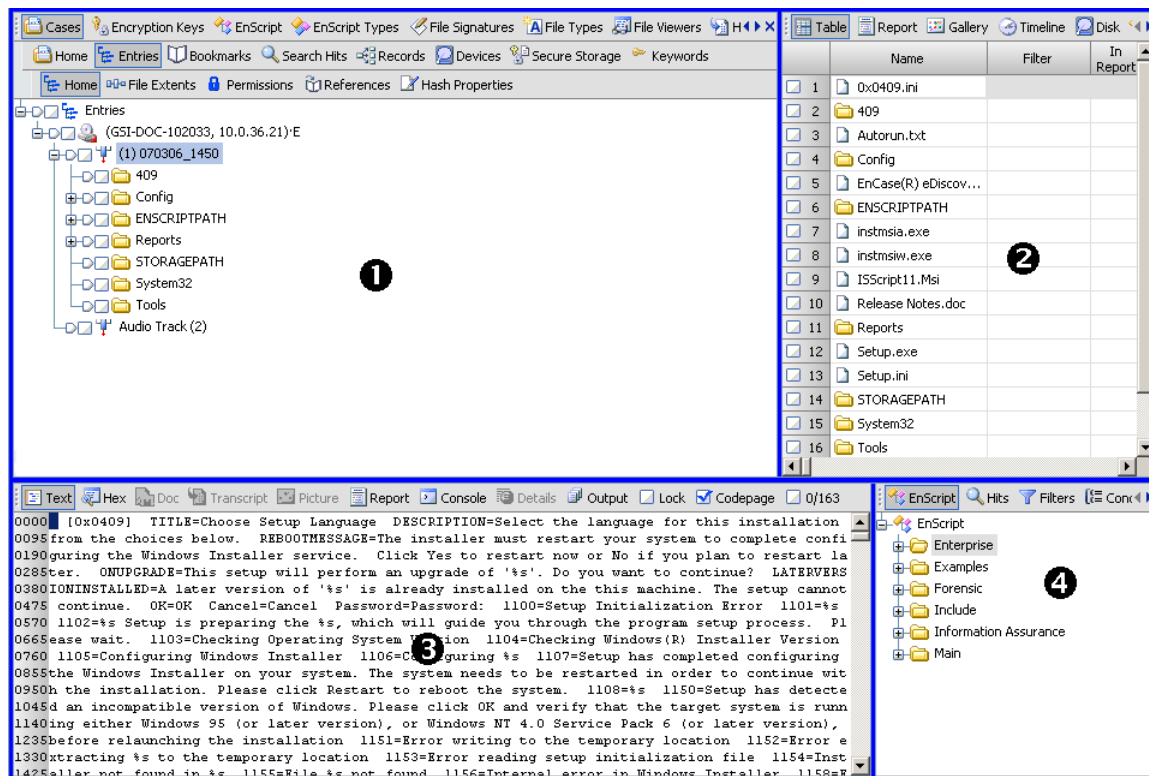
## Panes

Most EnCase work is done from one of the panes in the main display. The current display contains four panes containing different data and displays.

These include the following:

- **Tree pane** shows case- associated data in a tree format.
- **Table pane** presents a tabular data list that varies depending on various selections.
- **View pane** presents facsimiles of selected data. It varies depending on selections.
- **Filter pane** shows filter lists.

Figure 7 Panes as they appear in the main window showing 1) Tree pane, 2) Table pane, 3) View pane 4) Filter pane.



You can separate each pane from the main window and display them as individual windows.

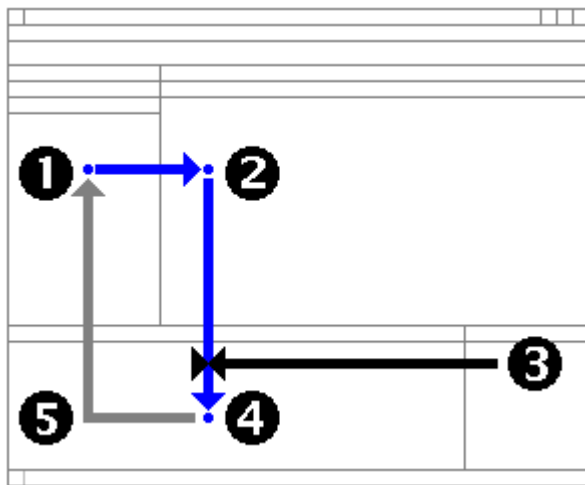


## Panes in the Analysis Cycle

Panes drive and organize the evidence analysis cycle.

The evidence cycle is where you define your investigation of acquired evidence. Analysis of evidence is cyclical, because you will redefine selection and processing as your analysis requirements evolve during the investigation.

*Figure 8 Panes in the Analysis Cycle, where 1) container entries selected in the Tree pane determine the contained entries that appear in the Table pane, 2) contained entries selected in the Table pane determine the contents that appear in the View pane, 3) optionally, filters, searches, and processing defined in the Filters pane narrow the contents or results of the analysis that appear in the View pane, 4) results of the current analysis cycle, and 5) subsequent refinements of the analysis.*



The tree pane provides you with the starting point of the analysis. This is where you select the container entries, such as devices and folders that contain the evidence you want to examine.

The Table pane presents the contents of the entries selected in the Tree pane. You can refine entries to be examined here.

The Filters pane gives you the means to search, filter, and automate the examination of the entries selected for examination in the Tree and Table panes. This narrows and focuses your analysis effort. The Filter pane provides tabs that enable you to view analytical results in places other than the View pane.

The View pane provides various tools that help you explore and see the results of the analysis. If the results of the analysis are sufficient for your purposes, the analysis can move on to other aspects of the investigation. If not, the analysis can be redefined and performed again.

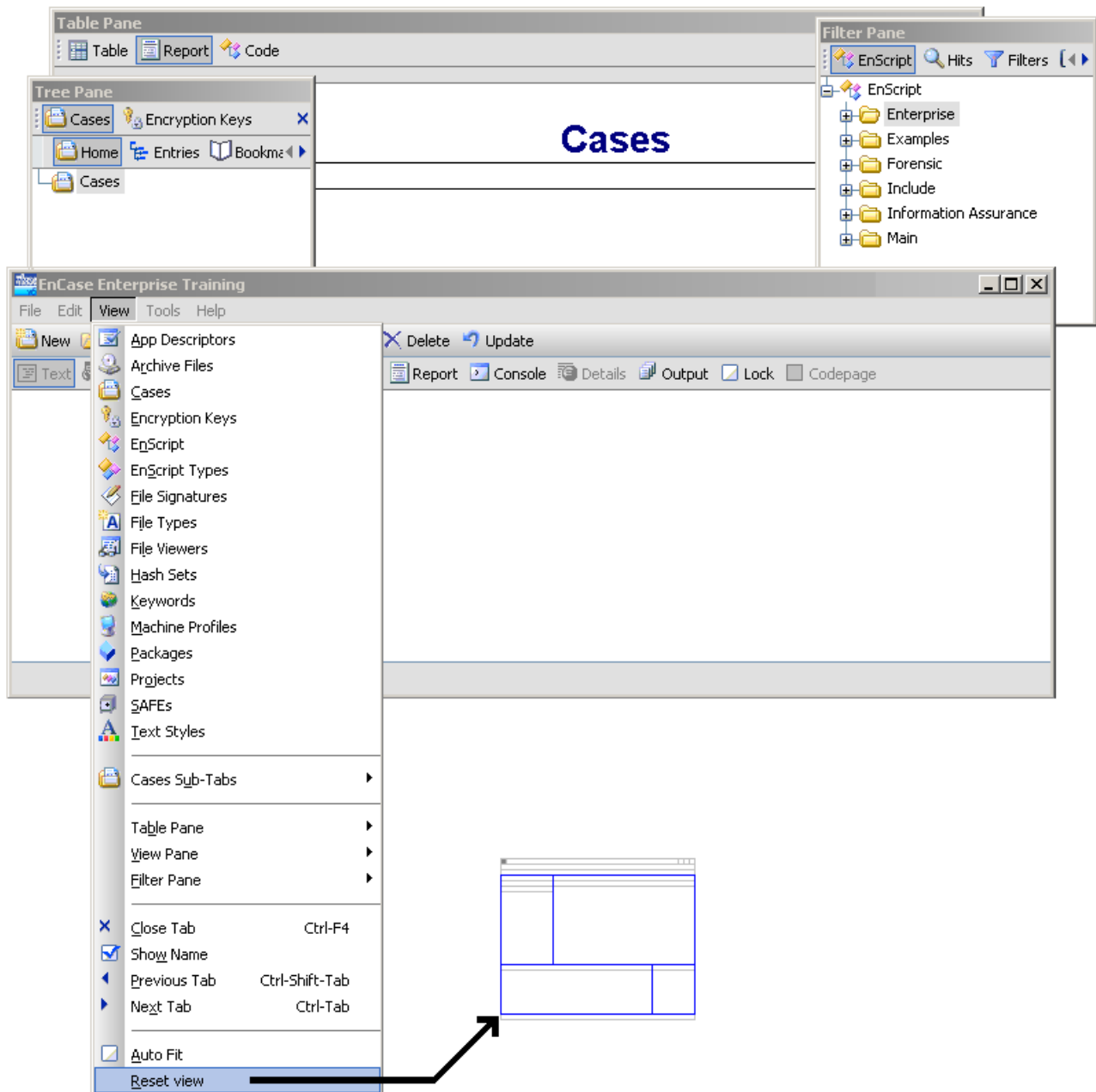
## Panes as Separate Windows

The individual panes that appear in the main window can be displayed in separate windows.

In the main window, each pane has a drag handle. You can drag the pane outside the main window and the pane will appear in a secondary window. Once three panes are dragged from the main window, the remaining pane does not display a drag handle and remains associated with the main window. The panes cannot be dragged back into the main window.

Refreshing the view displayed in the main window places all the panes back in the main window in their usual location.

Figure 9 Panes appearing as secondary windows, showing the Tree pane, Table pane, and Filter pane as separate windows. The View pane appears in the main window where the Reset view command is selected from the View menu. The Reset view command puts the panes appearing in separate windows back into the main window.



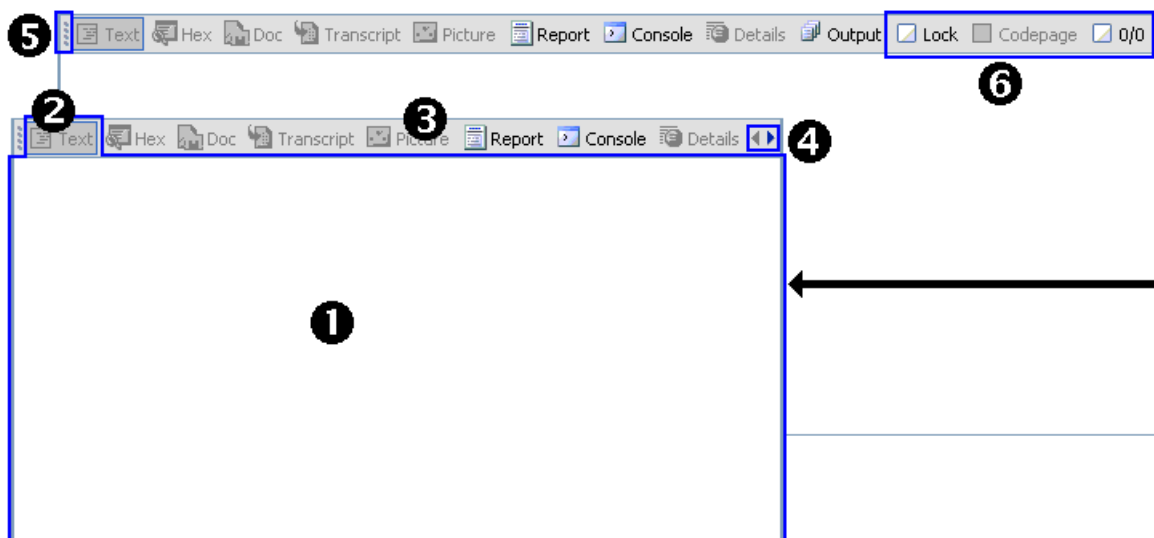
## Pane Features

Use pane features while working with panes and their tabs.

Each pane can display these features:

- Tabs and tab bar
- Scrollbar in the tab bar for a resized pane
- Controls in the tab bar
- Grab handle

Figure 10 Pane Features, where 1) is a View pane, 2) is the current tab, 3) is the tab bar, 4) is the scroll icon for navigating the tab bar, so that the tab you want to use can be displayed, 5) is the drag handle used to drag the pane out of the main window, so it appears in a secondary window, and 6) care commands controlling the tab bar.



Each pane contains one or more tabs.

As the main window is resized, the tab toolbar resizes correspondingly. When a pane is resized to a size not as wide as its toolbar, the tabs are hidden and a scroll icon appears. The scroll icon lets you scroll to the right or left so you can view the hidden tabs. You can wrap the tabs, rather than having them hidden, by using **AutoFit** on the right-click menu of the tab toolbar.

The tab toolbar may contain controls in addition to tabs. The scrollbar exposes these controls as well as tabs when either is hidden.

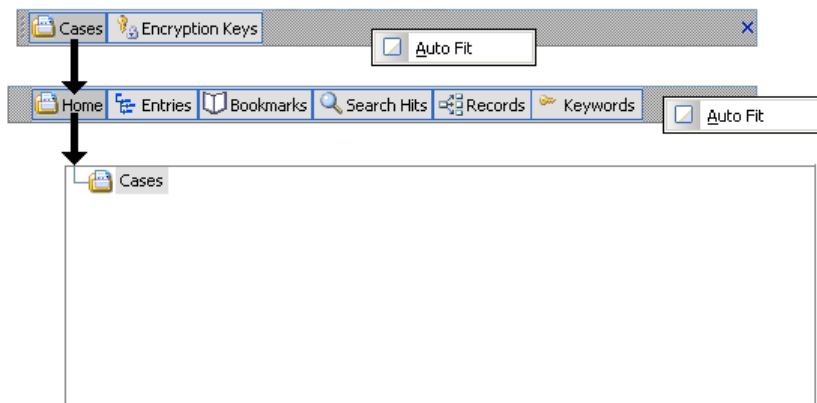
Each tab also has a grab handle used to move the tab outside the main window where it appears in a secondary window. Once three tabs are removed from the main window, the last tab in the main window no longer displays a grab handle, because it cannot be removed from the main window.

## Pane Tab Bar and Pane Tab Bar Menu

Each pane contains one or more tabs. Clicking a tab displays different content in the pane. Tabs are organized into a tab bar. Tabs may contain sub-tabs, and these are organized by separate tab toolbars.

Each tab bar has its own menu. The menu displays when you right click the tab bar.

*Figure 11 Pane Tab Bars and their Tab Bar Menus. The tab bars have been darkened where the menu can be displayed. The tabs have their own menus. Tabs were closed on the second tab bar to shorten it.*



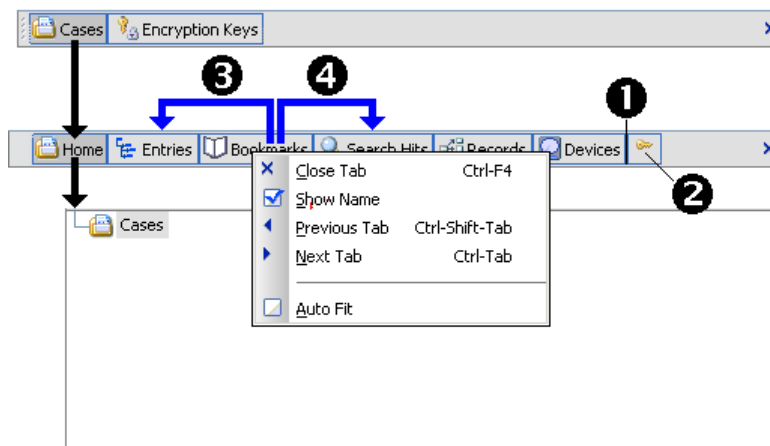
**Auto Fit** toggles whether the tab bar displays as a single row with a scrollbar, or wrapped to multiple rows when the pane is resized.

## Tab Right-Click Menu

Each tab or sub-tab displays the same right-click menu.

This menu manages tabs and provides another way of moving from one tab to another. The tab toolbar menu command **Auto Fit** is also available here.

Figure 12 The right-click menu, where 1) indicates that you closed a tab, 2) indicates a tab displaying only the icon, with the name hidden, 3) the Previous tab , and 4) the Next tab.



**Close Tab** hides a tab and its associated data. To display the data after closing a tab, use the View menu command associated with the tab (for example, **View > Cases Sub-Tabs > Secure Storage** reopens the Secure Storage sub-tab).

**Show Name** toggles the text displaying the name of the tab. When the text is hidden, the icon is still displayed. You can shorten the contents of the tab bar by hiding the name text.

**Previous Tab** displays the tab to the left of the current tab on the tab bar.

**Next Tab** displays the tab to the right of the current tab on the tab bar.

**Auto Fit** toggles whether the tab bar is displayed as a single row with a scrollbar, or wrapped to multiple rows when the pane is resized.

## Individual Panes

The individual panes that comprise the main window are:

- Tree pane
- Table pane
- View pane
- Filters pane

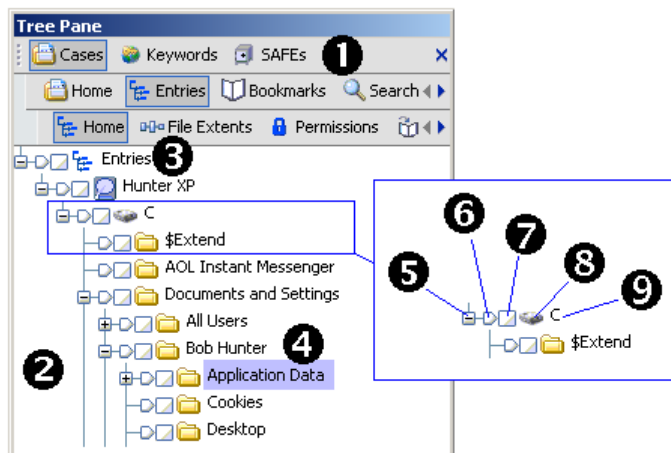
## Tree Pane

The Tree pane establishes the context for all case data analysis.

The Tree pane organizes a collection of tabs that contain a tree specific to that tab. A tree represents the hierarchical structure of a related collection of entries or objects .

The very first object in a tree is the root. Folder objects contain other folder objects. Non-folder, terminal, leaf objects do not appear in the tree. They appear in the Table pane when their containing folder object is highlighted.

*Figure 13 A Tree Pane, as a window, along with its 1) tab bars and its 2) tree, where Entries is the root of the tree, Hunter XP is a device, C is a volume, and the rest of the tree consists of folders. In the tree, 4) Application Data is highlighted. Each object in the tree can consist of 5) an Expand/Collapse icon, as seen when expanded, 6) a Set All icon, 7) a Checkbox, 8) a Category icon, and 9) a Name.*



A single entry or object in the tree consists of the following:

**Expand/Collapse** determines if the contained entries or objects are displayed or are hidden. Where a folder object appears that does not have an **Expand/Collapse** icon, the entries or objects it contains appear in the table in the Table pane, instead of the tree.

**Set Include** determines whether the entry or object and the entries and objects it contains appear in the Table pane where the entries can be selected for further analysis or exploration.

**Checkbox** enables you to select the entry or object without selecting the entries of objects it contains.

**Category** indicates the type of entry.

**Name** contains and displays the name of the entry or object. The name can be highlighted, which indicates that the entries or objects contained in the entry or object associated with the name appear in the Table pane.

Clicking on any part of a entry or object highlights it.



## Table Pane

The Table pane contains tabs that show you different aspects of the objects selected in the Tree pane.

Selecting a tab determines the representation used. The Table tab of the Table pane displays information about these entries in a numbered table. Except for the Gallery tab, this information is descriptive, rather than the actual content of the entries. You can view and further explore the content you select in the Table pane.

Figure 14 The Table pane lists the data from the object selected in the Tree pane, where 1) the tab toolbar contains tabs appropriate for the type of data you selected in the Tree pane, and 2) the column headers show you the values you can use in the analysis (for example, a column header for files is File Type), 3) the numbered selection column where you select the table entries to use in operations, and 4) a highlighted entry.

The screenshot shows the 'Table Pane' window with a tab toolbar at the top. The 'Table' tab is selected. The table below lists file entries with columns for Name, Filter, In Report, File Ext, File Type, File Category, and Description. A numbered selection column (1) is on the left. Callout 2 points to the 'Name' header, callout 3 to the selection column, and callout 4 to the 'File Category' column.

	Name	Filter	In Report	File Ext	File Type	File Category	Description
1	Hunter Pics.Ink		No	Ink	Link	Windows	File, Archive
2	Removable Disk (C)...		No	Ink	Link	Windows	File, Archive
3	Sabrina Dewercs.Ink		No	Ink	Link	Windows	File, Archive
4	session.log.Ink		No	Ink	Link	Windows	File, Archive
5	download.Ink		No	Ink	Link	Windows	File, Archive
6	Hunter.log.Ink		No	Ink	Link	Windows	File, Archive
7	X Drive.txt.Ink		No	Ink	Link	Windows	File, Archive
8	Sample Pictures.Ink		No	Ink	Link	Windows	File, Archive
9	Q309521.log.Ink		No	Ink	Link	Windows	File, Archive
10	WINDOWS.Ink		No	Ink	Link	Windows	File, Archive
11	101-0174_IMG.JPG...		No	Ink	Link	Windows	File, Archive
12	103-0396_IMG.JPG...		No	Ink	Link	Windows	File, Archive
13	Christina Detsiwt.Ink		No	Ink	Link	Windows	File, Archive
14	Desktop.ini		No	ini	Initialization	Windows	File, Hidden, System, Ar...
15	X Drive.txt (2).Ink		No	Ink	Link	Windows	File, Archive
16	Special Interests - ...		No	Ink	Link	Windows	File, Archive
17	101-0184_IMG.JPG...		No	Ink	Link	Windows	File, Archive
18	Sabrina and Christi...		No	Ink	Link	Windows	File, Archive
19	Chaser1191.Ink		No	Ink	Link	Windows	File, Archive
20	receive.Ink		No	Ink	Link	Windows	File, Archive

## Sorting a Table

You can sort up to five columns of a table in the Table pane.

You can do this in two ways:

- Double-clicking on the column header
- Using the Sort command on the table's right-click menu

A single red triangle appears in the column header when sorting a single column, and to indicate the primary sort when you sort by more than one column.

To sort by multiple columns, after the primary sort, press the shift key while double-clicking the desired additional column headers. Two red triangles appear in the header of the second column sorted. Three red triangles appear for the third column sorted, with four in the fourth, and five in the fifth.

*Figure 15 A table with five sorted columns, where the columns are sorted in the following order: File Type, File Category, Signature, Description, and Last Accessed.*

	In Report	File Ext	File Type ▲	File Category ▲▲	Signature ▲▲▲	Description ▲▲▲▲	Is Deleted	Last Accessed ▲▲▲▲▲	File Created
<input checked="" type="checkbox"/> 1		rnd				File, Archive		04/30/07 03:18:33PM	09/10/06 11:59:33
<input checked="" type="checkbox"/> 2		L01				File, Archive		04/30/07 03:18:36PM	09/13/06 05:21:36
<input checked="" type="checkbox"/> 3						Folder		05/17/07 09:19:03AM	09/10/06 11:59:33

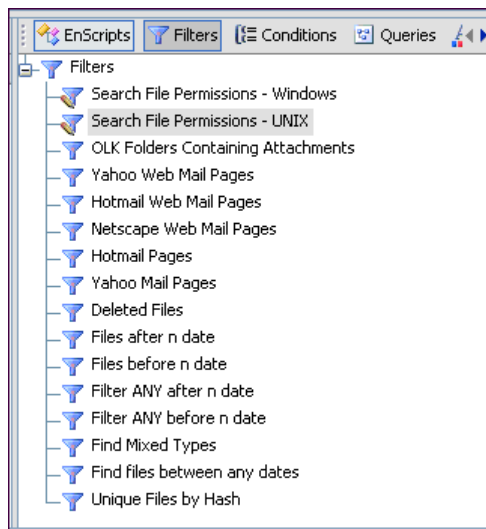
These methods work for all tables regardless of where they appear in the interface, not just tables in the Table pane.

## Filters Pane

The Filters pane contain the following tabs:

- EnScript
- Filters
- Conditions
- Queries
- Text Styles

These tabs organize analytic processes applied to the entries shown in the Table tab.



## Filtering Effects in Table Pane

When a filter is run, a query icon appears on the main menu bar, and the filter results show in the Table pane.

Query					
Table Report Gallery Timeline Disk Code					
	Name	Filter	Is Deleted	Last Written	File Created
<input checked="" type="checkbox"/> 1	_ORTRAIT.JPG	Deleted Files	Yes	04/30/00 04:19:38PM	01/28/05 08:05:08AM
<input checked="" type="checkbox"/> 2	_KSHIFT.JPG	Deleted Files	Yes	04/30/00 04:19:46PM	01/28/05 08:05:02AM
<input checked="" type="checkbox"/> 3	microprinting.jpg	Deleted Files	Yes	04/30/00 04:19:48PM	01/28/05 08:04:58AM
<input checked="" type="checkbox"/> 4	_UMBERS.JPG	Deleted Files	Yes	04/30/00 04:19:54PM	01/28/05 08:05:04AM
<input checked="" type="checkbox"/> 5	linesmoire.jpg	Deleted Files	Yes	04/30/00 04:19:56PM	01/28/05 08:04:52AM
<input checked="" type="checkbox"/> 6	_EAL.JPG	Deleted Files	Yes	04/30/00 04:20:00PM	01/28/05 08:05:24AM
<input checked="" type="checkbox"/> 7	fedreserveandtre...	Deleted Files	Yes	01/06/01 11:49:58PM	01/28/05 08:04:46AM
<input checked="" type="checkbox"/> 8	portrait1.jpg	Deleted Files	Yes	01/06/01 11:49:58PM	01/28/05 08:05:10AM
<input checked="" type="checkbox"/> 9	fedreserveandtre...	Deleted Files	Yes	01/06/01 11:49:58PM	01/28/05 08:04:48AM
<input checked="" type="checkbox"/> 10	_ORDER.JPG	Deleted Files	Yes	01/06/01 11:50:04PM	01/28/05 08:04:42AM
<input checked="" type="checkbox"/> 11	serialnumbers.jpg	Deleted Files	Yes	01/06/01 11:50:04PM	01/28/05 08:05:28AM
<input checked="" type="checkbox"/> 12	raisednoteten.jpg	Deleted Files	Yes	01/07/01 12:01:00AM	01/28/05 08:05:14AM
<input checked="" type="checkbox"/> 13	Counterfeit_finepri...	Deleted Files	Yes	01/07/01 12:06:08AM	01/28/05 08:04:44AM
<input checked="" type="checkbox"/> 14	Mellon.GIF	Deleted Files	Yes	01/07/01 12:11:58AM	01/28/05 08:04:56AM
<input checked="" type="checkbox"/> 15	_EAL-1.GIF	Deleted Files	Yes	01/07/01 12:12:00AM	01/28/05 08:05:18AM
<input checked="" type="checkbox"/> 16	_EAL-2.GIF	Deleted Files	Yes	01/07/01 12:12:10AM	01/28/05 08:05:20AM
<input checked="" type="checkbox"/> 17	_TRONG.GIF	Deleted Files	Yes	01/07/01 12:12:16AM	01/28/05 08:05:32AM
<input checked="" type="checkbox"/> 18	_RANK2.JPG	Deleted Files	Yes	01/07/01 12:25:06AM	01/28/05 08:04:50AM































The **Query** icon in the top menu bar appears with the filter results. When the icon shows a green +, filtered lists appear. If more than one filter has been run, its name appears, with ORed logic, in the table's **Filter** column.



When clicked, the **Query** icon changes its appearance and its associated list contents. As you can see below, the icon now has a – sign. In this state, the list shows selected evidence files and filtered files.



Here is a table display with the query in the – state.

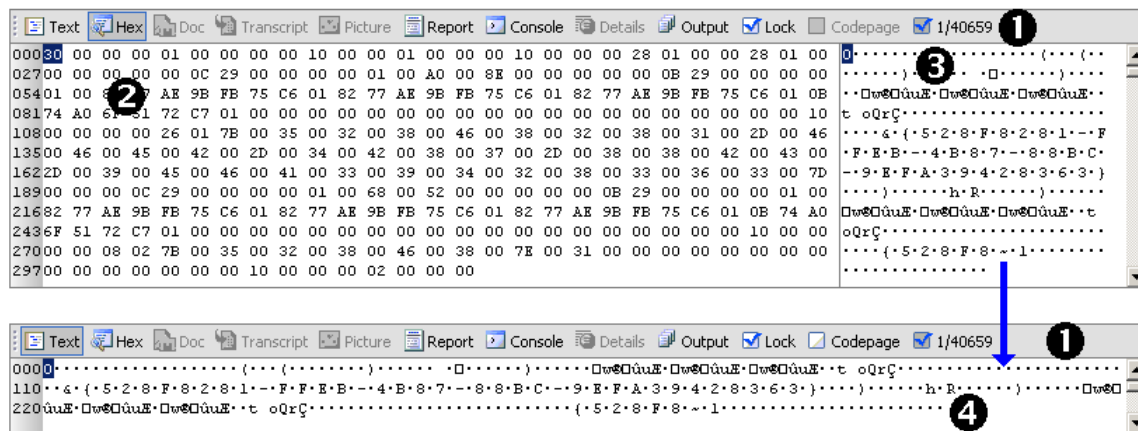
	Name	Filter	Is Deleted 	Last Written 	File Created
<input type="checkbox"/> 1	 WINK.GIF		No	04/30/00 03:18:06PM	01/28/05 08:04:36AM
<input type="checkbox"/> 2	 OLDBACK.JPG		No	04/30/00 03:22:34PM	01/28/05 08:04:32AM
<input type="checkbox"/> 3	 NEWBACK.JPG		No	04/30/00 03:22:36PM	01/28/05 08:04:30AM
<input type="checkbox"/> 4	 _ORTRAIT.JPG	Deleted Files	Yes	04/30/00 04:19:38PM	01/28/05 08:05:08AM
<input type="checkbox"/> 5	 _KSHIFT.JPG	Deleted Files	Yes	04/30/00 04:19:46PM	01/28/05 08:05:02AM
<input type="checkbox"/> 6	 microprinting.jpg	Deleted Files	Yes	04/30/00 04:19:48PM	01/28/05 08:04:58AM
<input type="checkbox"/> 7	 _UMBERS.JPG	Deleted Files	Yes	04/30/00 04:19:54PM	01/28/05 08:05:04AM
<input type="checkbox"/> 8	 linesmoire.jpg	Deleted Files	Yes	04/30/00 04:19:56PM	01/28/05 08:04:52AM
<input type="checkbox"/> 9	 _EAL.JPG	Deleted Files	Yes	04/30/00 04:20:00PM	01/28/05 08:05:24AM
<input checked="" type="checkbox"/> 10	 new100back.JPG		No	01/05/01 11:27:22PM	01/28/05 08:04:26AM
<input checked="" type="checkbox"/> 11	 bogusbill.jpg		No	01/06/01 10:51:48PM	01/28/05 08:04:18AM
<input checked="" type="checkbox"/> 12	 bogusbill1.jpg		No	01/06/01 10:52:22PM	01/28/05 08:04:22AM
<input type="checkbox"/> 13	 bogusbillstamped.jpg		No	01/06/01 10:53:08PM	01/28/05 08:04:24AM
<input type="checkbox"/> 14	 BINION.GIF		No	01/06/01 11:11:52PM	01/28/05 08:04:16AM
<input type="checkbox"/> 15	 1-28-SO.GIF		No	01/06/01 11:13:36PM	01/28/05 08:04:12AM
<input type="checkbox"/> 16	 fedreserveandrea...	Deleted Files	Yes	01/06/01 11:49:58PM	01/28/05 08:04:46AM
<input type="checkbox"/> 17	 fedreserveandrea...	Deleted Files	Yes	01/06/01 11:49:58PM	01/28/05 08:04:48AM
<input type="checkbox"/> 18	 portrait1.jpg	Deleted Files	Yes	01/06/01 11:49:58PM	01/28/05 08:05:10AM
<input type="checkbox"/> 19	 _ORDER.JPG	Deleted Files	Yes	01/06/01 11:50:04PM	01/28/05 08:04:42AM
<input type="checkbox"/> 20	 serialnumbers.jpg	Deleted Files	Yes	01/06/01 11:50:04PM	01/28/05 08:05:28AM
<input type="checkbox"/> 21	 raisednoteten.jpg	Deleted Files	Yes	01/07/01 12:01:00AM	01/28/05 08:05:14AM
<input type="checkbox"/> 22	 Counterfeit_finepri...	Deleted Files	Yes	01/07/01 12:06:08AM	01/28/05 08:04:44AM
<input type="checkbox"/> 23	 Mellon.GIF	Deleted Files	Yes	01/07/01 12:11:58AM	01/28/05 08:04:56AM
<input type="checkbox"/> 24	 _EAL-1.GIF	Deleted Files	Yes	01/07/01 12:12:00AM	01/28/05 08:05:18AM
<input type="checkbox"/> 25	 _EAL-2.GIF	Deleted Files	Yes	01/07/01 12:12:10AM	01/28/05 08:05:20AM
<input type="checkbox"/> 26	 _TRONG.GIF	Deleted Files	Yes	01/07/01 12:12:16AM	01/28/05 08:05:32AM
<input type="checkbox"/> 27	 _RANK2.JPG	Deleted Files	Yes	01/07/01 12:25:06AM	01/28/05 08:04:50AM
<input type="checkbox"/> 28	 Bits		No	01/28/05 08:04:42AM	01/28/05 08:04:40AM

## View Pane

The View pane contains tabs that display different views of the entry highlighted in the Table pane.

The View pane tabs display the content of the entry highlighted in the Table pane in different ways. Some of the tabs are more appropriate than others for certain kinds of data.

*Figure 16 Two View panes showing two ways to view the content: (top) the Hex tab and (bottom) the Text tab, where 1) are the tab toolbars, 2) is the hexadecimal view in the Hex tab, and 3) is the text view of the same object, and 4) is the text in the Text tab. Notice that the text representations in 3) and 4) are the same.*

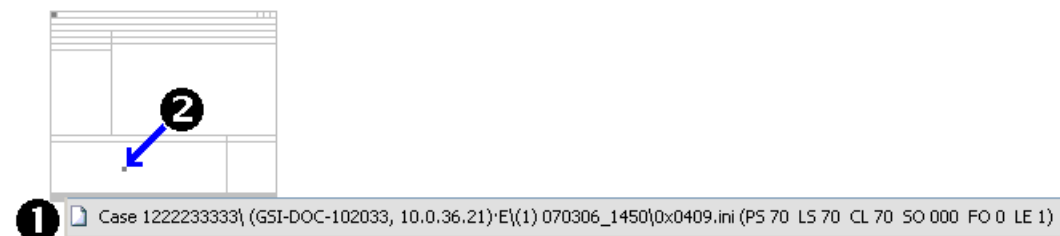


## Status Line

The status line provides details on the physical and logical drive location of a selection.

The status line displays at the bottom of the main window.

*Figure 17 The Status Line, where 1) is the status line, and 2) is the cursor in the View pane, driving the content of the status line.*



The file being examined in your EnCase® application drives some of the status line content. The location of the cursor in the content of the file being examined and content selected by the cursor also drives some of the status line content.

The status line content of the file being examined includes:

- Name of the case
- Name of the device
- Name of the volume
- Path to the file
- Filename

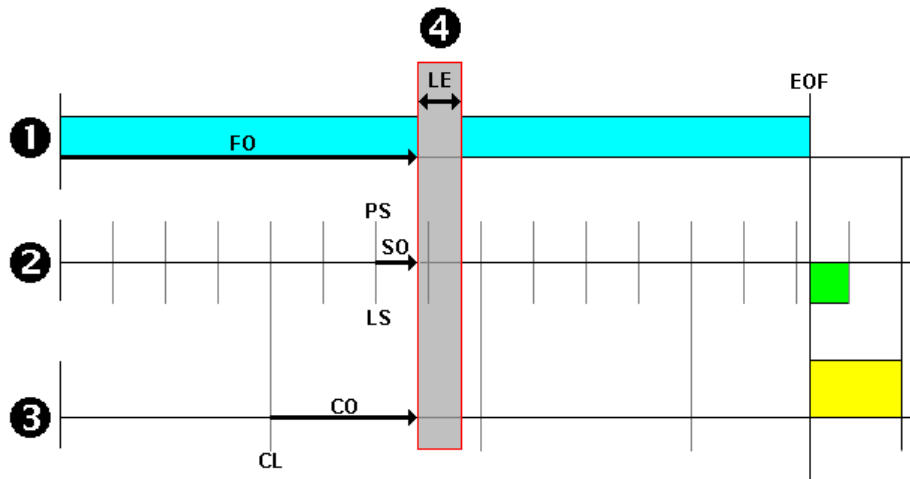
The status line content relative to the beginning of the file being examined includes:

- Physical sector (PS) displays the sector number of the physical sector relative to the beginning of the physical disk
- Logical sector (LS) displays the sector number of the logical sector relative to the beginning of the logical disk
- Cluster number (CL) displays the cluster number

The status line content relative to the location of the cursor within the file being examined includes:

- Sector offset (SO) displays the number of sectors, in bytes, between the start of the cluster and the current cursor location
- File offset (FO) displays the number of bytes between the start of the file and the current cursor location
- Length (LE) displays the length, in bytes, of the content currently selected by the cursor

Figure 18 Status line elements from drive geometry, where 1) is the content of a file from start to end of file (EOF), 2) sectors, 3) clusters, 4) width of the cursor. Notice that the physical sector (PS) value and the logical sector (LS) sector value are different, but address the same location.



## Panes and their Specific Tabs

The panes that comprise the main window organize collections of tabs.

They include:

- Tree pane tabs
- Table pane tabs
- View pane tabs
- Filters pane tabs



## Tree Pane Tabs

The Tree pane contains tabs with trees displaying many of the elements or objects used in your EnCase application.

Each tab contains a tree displaying a collection of elements in a hierarchy. For example, keywords you define appear in the Keywords tab. Keywords associated with the currently opened cases appear in the Cases-Keywords tab.

The elements found in these trees have unique right-click menus. The Edit menu matches the right-click menu of the currently selected element or object.

App Descriptors-Home	EnScript Types
App Descriptors-Hash Properties	File Signatures
Archive Files	File Types
Cases-Home	File Viewers
Cases-Entries-Home	Hash Sets-Home
Cases-Entries-File Extents	Hash Sets-Hash Items
Cases-Entries-Permissions	Keywords
Cases-Entries-References	Machine Profiles-Home
Cases-Entries-Hash Properties	Machine Profiles-Allowed
Cases-Bookmarks-Home	Packages
Cases-Search Hits-Home	Projects
Cases-Search Hits-Hash Properties	SAFEs-Home
Cases-Records-Home	SAFEs-Network
Cases-Records-Additional Fields	SAFEs-Roles
Cases-Devices-Home	SAFEs-Users
Cases-Devices-Acquisition Info	SAFEs-Events
Cases-Devices-Sources	Text Styles
Cases-Devices-Subjects	
Cases-Devices-Read Errors	
Cases-Devices-Missing Sectors	
Cases-Devices-Disk Elements	
Cases-Devices-CRC Errors	
Cases-Secure Storage	
Cases-Keywords	
Encryption Keys	
EnScript	

## Table Pane Tabs

The Table pane displays tabs that provide different views of the entries selected in the Tree pane.

The context established by the entries in the Tree pane determine what tabs appear in the Table pane. The Table, Report, and Code tabs appear in almost all contexts. Entries that involve time can appear in a Timeline tab. Where image content is involved, the Gallery tab is among the tabs that display.

Figure 19 Tabs that display in the Table pane, as determined by the Tree tab displayed in the Tree pane. Gray values mean that tab is available for use. White values mean that the tab is not available for use.

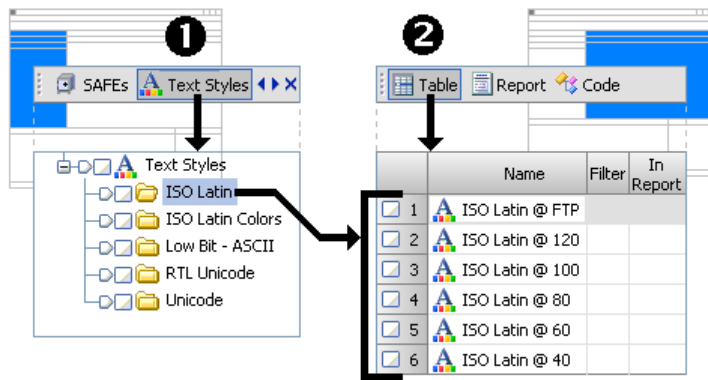
Selected Tree Pane Panel	Table Pane Panels				
	Table	Report	Gallery	Timeline	Code
App Descriptor-Home					
App Descriptor-Properties					
Archive Files					
Cases-Home					
Cases-Entries-Home					
Cases-Entries-File Extends					
Cases-Entries-Permissions					
Cases-Entries-References					
Cases-Entries-Hash Properties					
Cases-Bookmarks-Home					
Cases-Search Hits-Home					
Cases-Search Hits-Hash Properties					
Cases-Records-Home					
Cases-Records-Additional Fields					
Cases-Devices-Home					
Cases-Devices-Acquisition Info					
Cases-Devices-Sources					
Cases-Devices-Subjects					
Cases-Devices-Read Errors					
Cases-Devices-Missing Sectors					
Cases-Devices-Disk Elements					
Cases-Devices-CRC Errors					
Cases-Secure Storage					
Cases-Keywords					
Encryption Keys					
EnScript					
EnScript Types					
File Signatures					
File Types					
File Viewers					
Hash Sets-Home					
Hash Sets-Hash Items					
Keywords					
Machine Profiles-Home					
Machine Profiles-Allowed					
Packages					
Projects					
SAFEs-Home					
SAFEs-Network					
SAFEs-Roles					
SAFEs-Users					
SAFEs-Events					
Text Styles					

Content displayed in these tabs is determined by selections made in the tree of the tab displayed in the Tree pane.

When the Text Styles tab displays in the Tree pane, and you select the root of the Text Styles tree, the Table tab of the Table pane displays a table containing the same folders displayed in the tree.

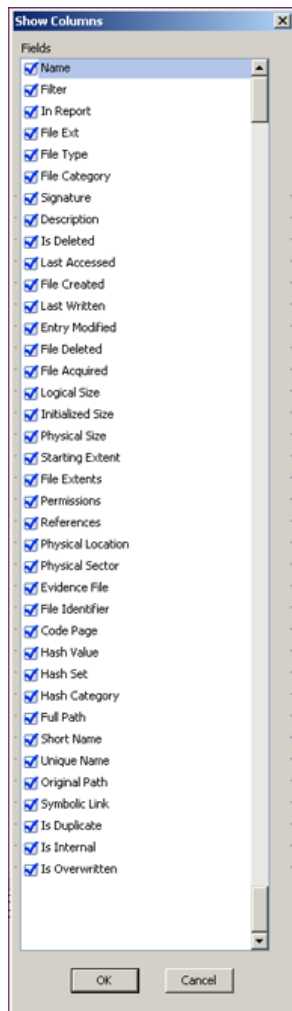
When a particular folder is selected in the tree, the contents of that folder appear in the Table tab of the Table pane.

Figure 20 Table Pane context, where 1) the object selected in the tree on the Text Styles tab of the Tree pane determines 2) the content displayed in the table in the Table tab of the Table pane.



## Table Tab Columns

Table tab columns are activated or deactivated by right-clicking the table tab, selecting **Show Columns** and selecting desired columns. By default, all columns are selected.



The figure below shows each column header. In order to fit them into the document they are stacked. In the EnCase Table pane, you scroll horizontally across the pane to see them. You can "drag and drop" columns to arrange them according to your needs. Each is described below.

Name	Filter	In Report	File Ext	File Type	File Category
Signature	Description	Is Deleted	Last Accessed	File Created	Last Written
Entry Modified	File Deleted	File Acquired	Logical Size	Initialized Size	Physical Size
Starting Extent	File Extents	Permissions	References	Physical Location	Physical Sector
Evidence File	File Identifier	Code Page	Hash Value	Hash Set	Hash Category
Full Path	Short Name	Unique Name	Original Path	Symbolic Link	Is Duplicate
Is Internal	Is Overwritten				

**Name** is the name of the entry. Icons to the left of the filename indicate the type of entry, such as device, folder, or document.

**Filter** displays the name of the saved filter options if the files meet the criteria set.

**In Report** indicates whether or not the item appears in the report. To include the file in a report, right-click the In Report column and select **In Report**, or select the entry and press Ctrl + R. To include more than one entry in the report, select each one in the first column checkbox, then right-click the In Report header and select **In Report**.

**File Ext** displays a file's extension, such as .exe, .jpg, or .doc.

**File Type** names the file type. The software generates this information from the File Types table using the file's extension. When you run a Signature Analysis, this information is generated from the file's identifying (header) information inside the file.

**File Category** classifies the entry as Windows, database, picture, etc.

**Signature** identifies the file by header, not file extension. See Analyzing and Searching Files, for more information on using file signatures.

**Description** gives a short explanation of the entry (also indicated by the icon to the left of the file name).

**Is Deleted** displays **TRUE** if the file is deleted but not emptied from the Recycle Bin.

**Last Accessed** displays the date of the last activity of the file. A file does not have to be altered for the **Last Accessed** date to change—only accessed. Any activity (such as viewing, dragging, or even right-clicking) may change the **Last Accessed** date. The last accessed date may also change if the file is accessed by a program such as a virus checker.

**File Created** is a record of when a particular file was created at that location. If a file is edited and changed on January 3, then copied to a floppy diskette on January 15, and that floppy diskette is acquired on January 28, the entry shows that the file on the floppy disk was created after it was last written to or accessed.

**Last Written** displays the last date and time a file was opened, edited, and then saved. If a file is opened then closed, but not altered, the **Last Written** date does not change.

**Entry Modified** refers to the file entry pointer and its information, such as file size. If a file was changed but its size not altered, the **Entry Modified** date does not change.

**File Deleted** shows the deletion time and date. If an entry in an INFO2 file on an NTFS volume has a deleted date, **TRUE** appears in the **Is Deleted** column.

**File Acquired** displays the date and time the evidence file, in which the selected file resides, was acquired.

**Logical Size** displays the byte size of the file.

**Initialized Size** is the size of the file when it is opened. This applies only to NTFS file systems.

**Physical Size** is the cluster size occupied by the file, that is the physical disk space used by the file. Given a cluster size of 4096 bytes, the physical size of any file with a logical size less than 4096 bytes has a physical size of 4096 bytes. A file with just one more byte, 4097 bytes, for example, requires two clusters, or 8,192 bytes of physical disk space. The 4095 byte difference in the second cluster is called **slack space**.

**Starting Extent** shows the starting cluster of every file in the case. The format displayed is evidence file number, logical drive letter, cluster number. For example, a starting extent of 1D224803 means that the file is on the second evidence file (counting begins at zero), on the logical D:\ drive, at cluster 224803.

**File Extents** lists the number of extents a fragmented file occupies on a drive. To view extents, click the column value of the file being examined, and select the Details tab of the Report pane. You can also select the file in Table pane, then select the **File Extents** sub-tab, above the Tree pane.

**Permissions** displays security settings of a file or folder. **TRUE** indicates a security setting is applied. To view security settings, select the entry and click on the Details tab in the lower pane. Or you can select the file in the Entries table, then select the **View > Cases Sub-Tabs > Entries Sub-Tabs > Permissions** menu to display the Permissions in the Table pane.

**References** is the number of times the file has been referenced in the case. For example, if you bookmark a file three times, the references column shows that.

**Physical Location** the number of bytes into the device at which that unallocated cluster begins. The program organizes device unallocated clusters into one virtual file. It reads the file system's File Allocation Table (FAT), or the NTFS Bitmap, to create this virtual file. This allows the examiner to efficiently examine unallocated clusters.

**Physical Sector clusters. Physical** lists the starting sector where the item resides in unallocated space.

**Evidence File** is the name of the root evidence file where the entry in the table resides.

**File Identifier** is a file table index number stored in the master file table. It is a unique number allocated to files and folders in an NTFS file system.

**Code Page** is the character encoding table upon which the file is based.

**Hash Value** displays the hash value of every file in the case. You must run the **Compute Hash Value** command to generate this information.

**Hash Set** displays the hash set to which a file belongs. If no hash sets are created or imported, the column is unpopulated.

**Hash Category** displays the hash category to which a file belongs. If no hash sets are created or imported this column is unpopulated.

**Full Path** displays the file location within the evidence file. The evidence file name is included in the path.

**Short Name** is the name Windows assigns using the DOS 8.3 naming convention.

**Original Path** displays information derived from the INFO2 file for deleted files that are in the Recycle Bin. The path is where the deleted file was originally stored.

- ☐ The column is blank for undeleted files.
- ☐ The original location is shown for files in the Recycle Bin.
- ☐ Shows what file has overwritten the original file for deleted and overwritten files

**Symbolic Link** can provide links to directories or files on remote devices.

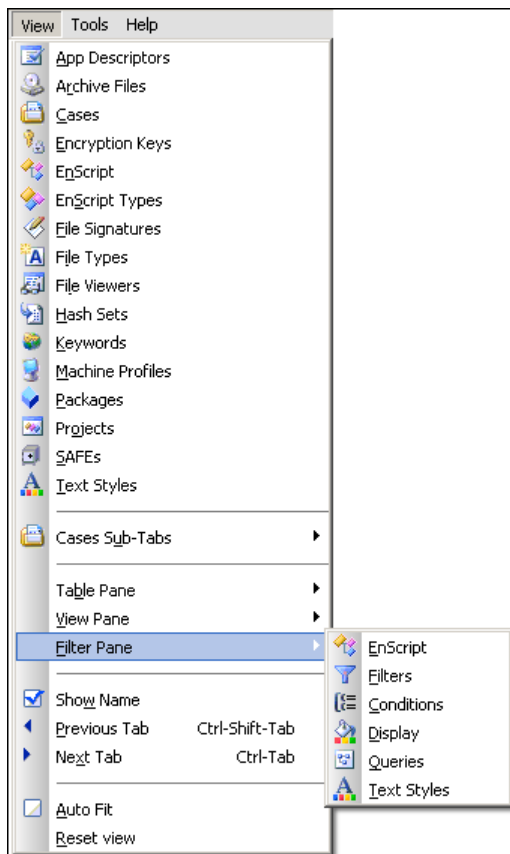
**Is Duplicate** displays **TRUE** if the displayed file is a duplicate of another.

**Is Internal** references hidden files the OS uses internally but are hidden from the user.

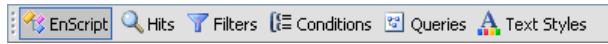
**Is Overwritten** displays **TRUE** if the original file is deleted and its space is occupied by another file.

## Filters Pane Menu

Selecting a Filters pane menu tab displays filters features.



The menu that appears above the Filter pane shows the same tab options. These are described here.



Clicking a tab changes the contents of the Filters pane as follows:

- **EnScript** displays an EnScript tree menu.
- **Filters** displays all available filters.
- **Conditions** displays all available conditions.
- **Display** shows filters, conditions and queries that are running.
- **Queries** displays tree menu of available conditions.
- **Text Styles** provides access to available text styles.

## View Pane Tabs

The View pane tabs display different representations of the entries selected in the Table pane.

When the type of view is appropriate for the selected entry in the Table pane, the View pane tab is enabled.





The View pane accesses the following tabs:

- Text
- Hex
- Doc
- Transcript
- Picture
- Report
- Console
- Details
- Output

The tabs on the View pane cannot be closed.

The tab bar for the View pane also contains controls specific to the View pane. These controls include:

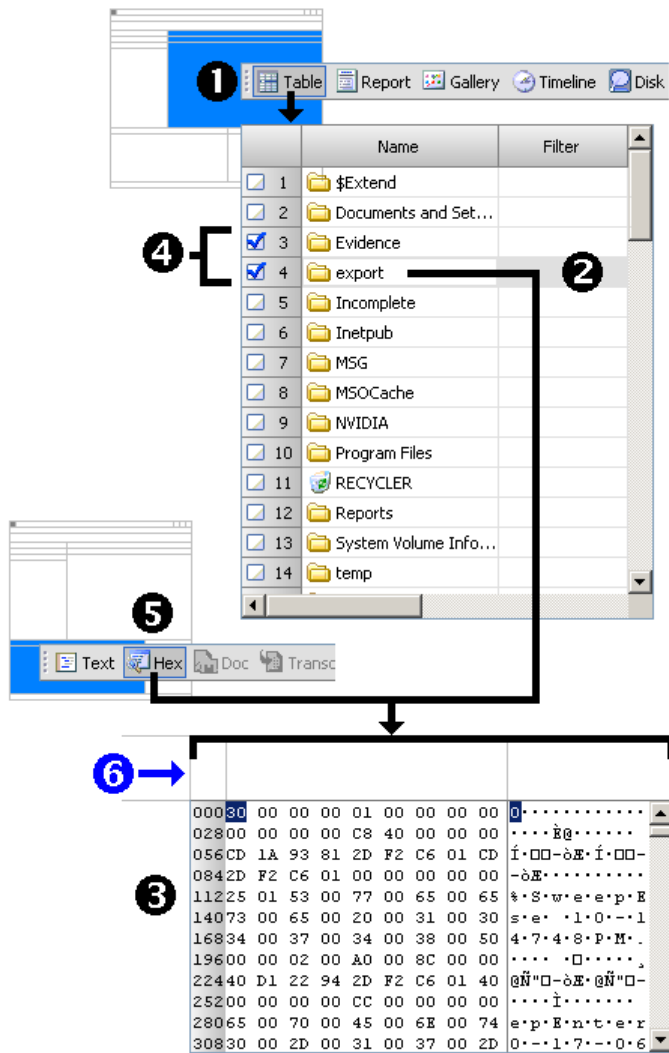
**Lock** prevents the tab from changing if the file type of the file selected in the Table pane changes. By default, the View pane displays the appropriate tab for the type of file selected in the Table pane. This behavior is overridden when **Lock** is selected. When you select **Lock**, the currently displayed tab type is retained, even if the selected file type in the Table pane changes. For example, if you Lock the View pane with the Picture tab in view and then select entries in the Table pane that do not contain images, the Picture tab may show nothing.

**Codepage** determines whether the detected, rather than the default, codepage is used in tabs that display text.

**Selected/Total** displays the number of entries selected as a fraction of the total number of entries available in the current case.

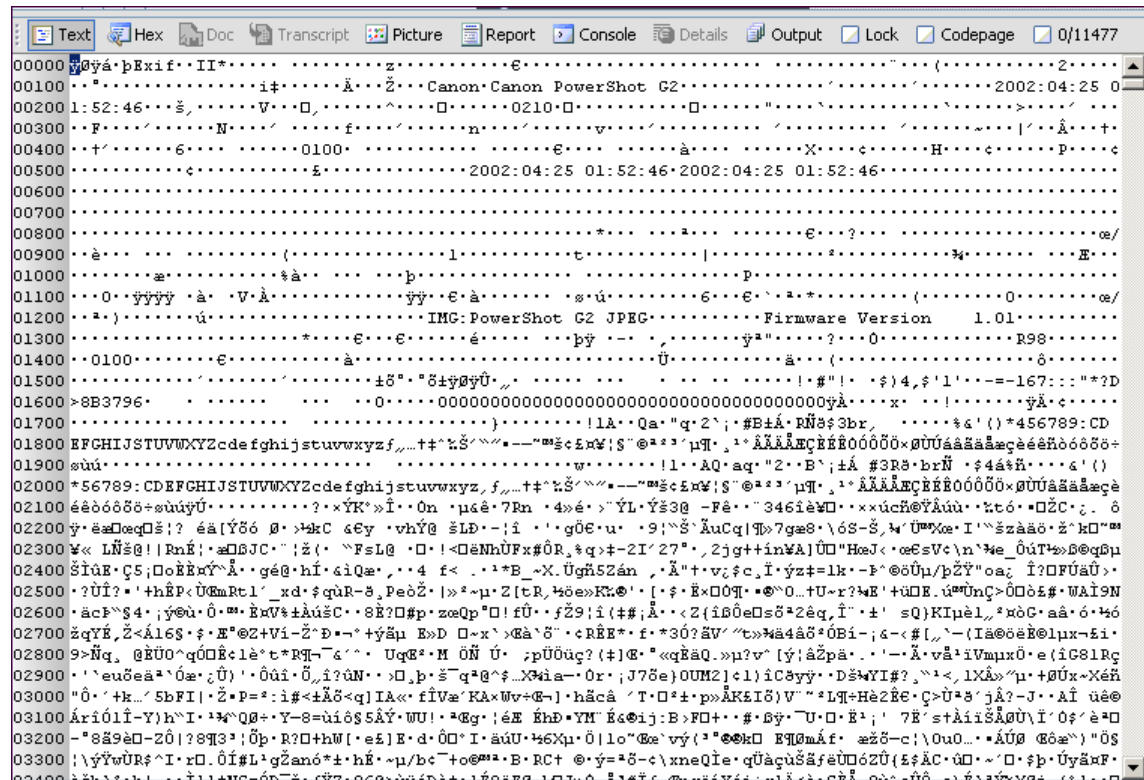
The context established by selecting an entry in the Table pane determines what content is displayed in the View pane. The View pane displays the content of one entry from the table. While several entries can be blue checked in the Table pane, only one entry can be highlighted at a time.

Figure 21 View pane context, where 1) the Table pane contains a table where only one entry can be 2) highlighted for further exploration in 3) a tab in the View pane. 4) Checking table entries does not drive the content displayed in the tab displayed in the View pane. The representation of the highlighted content is made when you 5) select the desired View pane tab. 6) The Hex tab contains a representation consisting of an address, the numeric byte values, and the text representation of those numeric byte values.



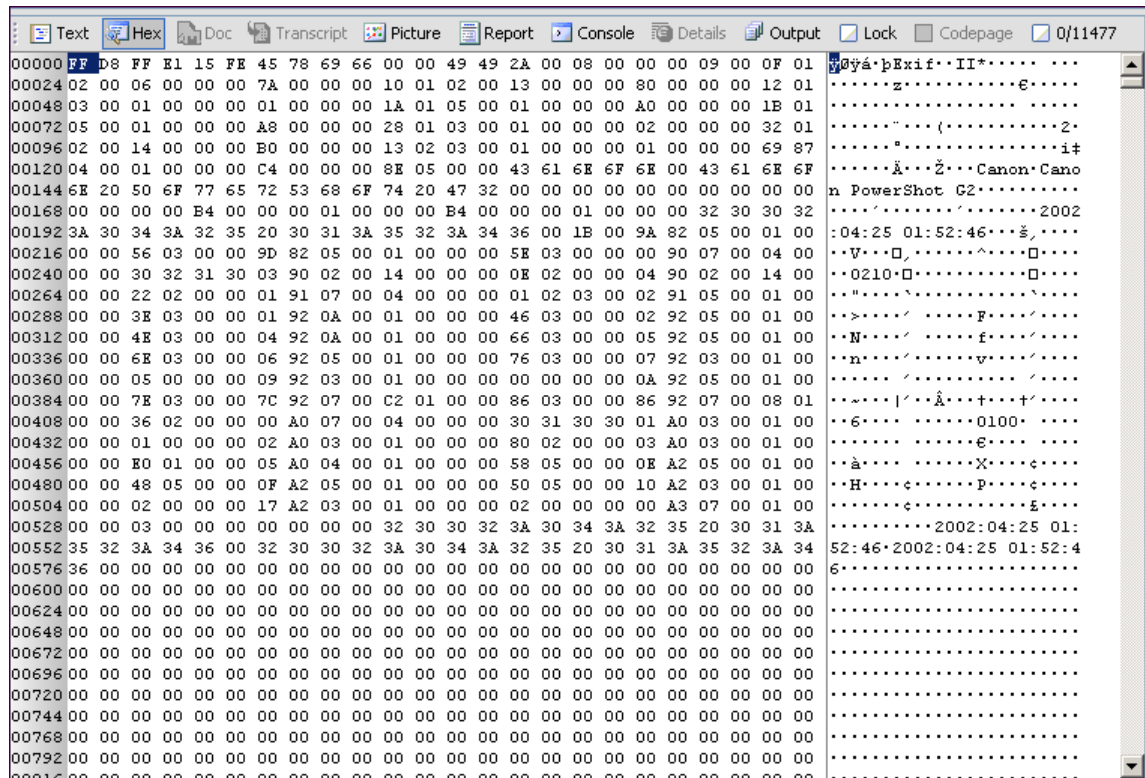
## The Text Tab

The Text tab shows the highlighted file as ASCII text.



## The Hex Tab

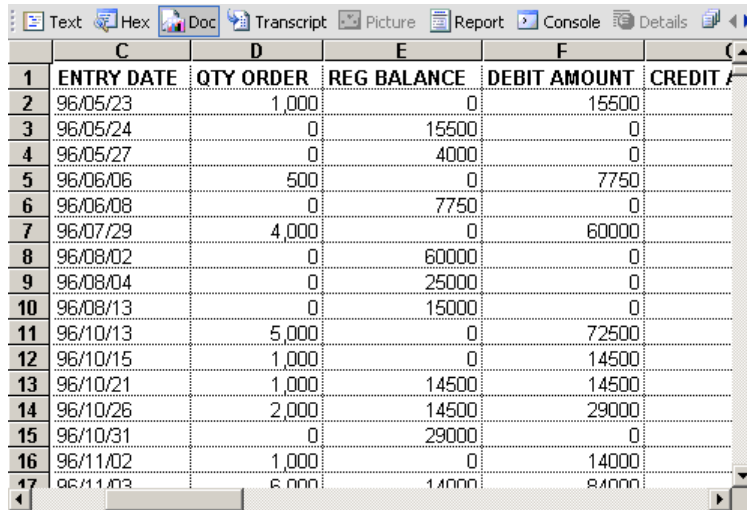
The Hex tab shows a split view of a file with hexadecimal values on the left and ASCII on the right.



## The Doc Tab

The Doc tab of the View pane uses Oracle Outside In technology to display text in its native format.

This viewer technology provides application software developers with high-fidelity document viewing without having to use native applications for more than 390 file formats on Windows platforms.

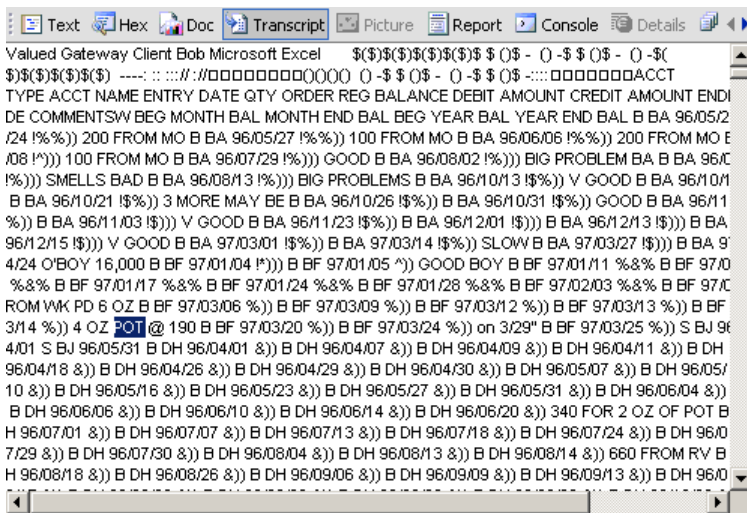


	C	D	E	F	
	ENTRY DATE	QTY ORDER	REG BALANCE	DEBIT AMOUNT	CREDIT #
2	96/05/23	1,000	0	15500	
3	96/05/24	0	15500	0	
4	96/05/27	0	4000	0	
5	96/06/06	500	0	7750	
6	96/06/08	0	7750	0	
7	96/07/29	4,000	0	60000	
8	96/08/02	0	60000	0	
9	96/08/04	0	25000	0	
10	96/08/13	0	15000	0	
11	96/10/13	5,000	0	72500	
12	96/10/15	1,000	0	14500	
13	96/10/21	1,000	14500	14500	
14	96/10/26	2,000	14500	29000	
15	96/10/31	0	29000	0	
16	96/11/02	1,000	0	14000	
17	96/11/03	6,000	14000	84000	

## The Transcript Tab

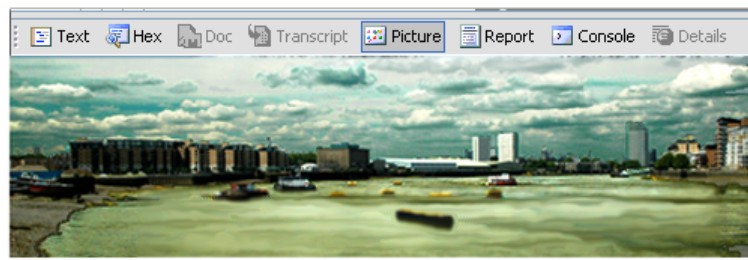
The Transcript tab uses Oracle Outside In technology to extract text from a file containing more than text.

The Transcript tab displays plain text content pulled from its non-plain text native format. This makes it especially attractive for creating sweeping bookmarks inside files that are not normally stored as plain text, such as Excel spreadsheets.



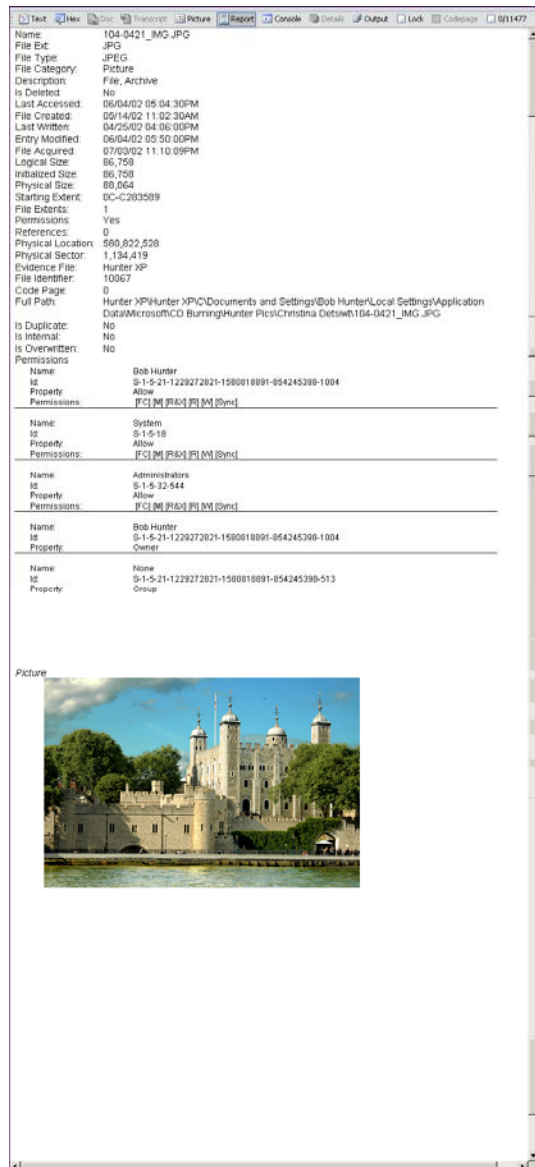
## The Picture Tab

The Picture tab of the View pane displays the contents of an image file.



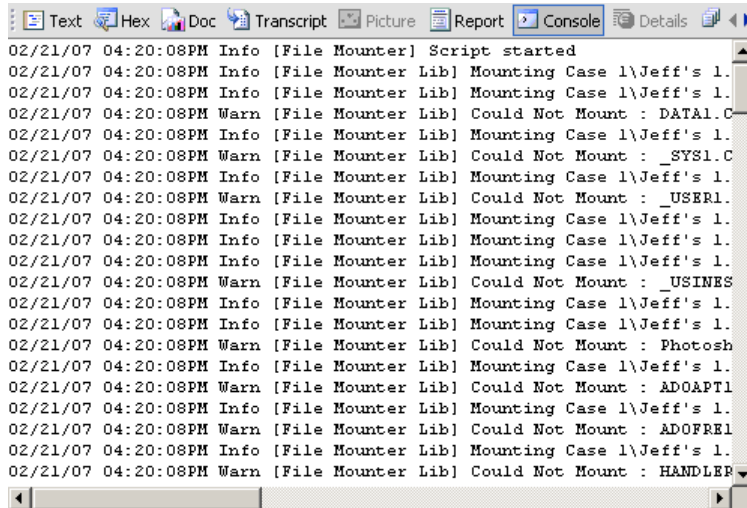
# The Report Tab

The Report tab displays a detailed list of file attributes in the View pane.



## The Console Tab

Use the Console tab to view output status messages when running EnScript® programs.



## The Details Tab

The Details tab provides file extent information.

To view file extents

1. Open a case and display its contents.
2. Scroll to the file extents column in the Table pane and click File Extents in some row.
3. Click the **Details** tab in the Reports pane to view the file extents.

The figure below shows the first eight file extents from a piece of evidence.

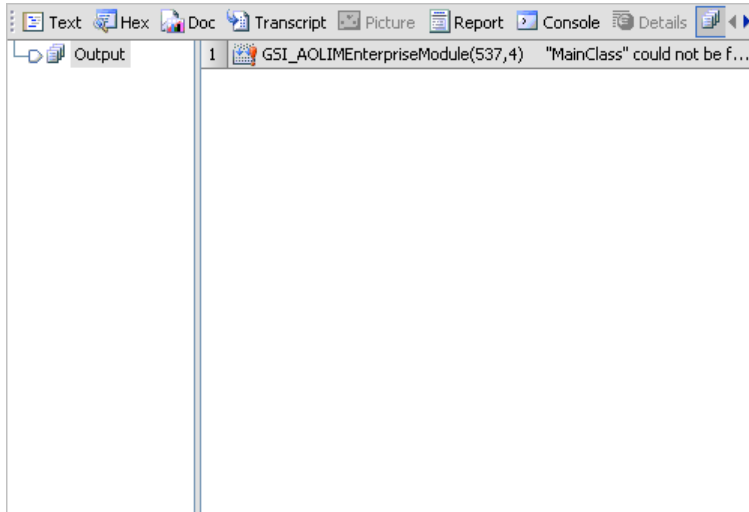
The screenshot shows the EnCase Forensic interface with the 'Details' tab selected. The 'File Extents' table is displayed with the following data:

	Start Sector	Sectors	Start Byte	bytes	Start Cluster	Clusters
1	52,411	16	26,834,432	8,192	13,087	4
2	64,187	4	32,863,744	2,048	16,031	1
3	104,651	4	53,581,312	2,048	26,147	1
4	115,663	4	59,219,456	2,048	28,900	1
5	143,947	4	73,700,864	2,048	35,971	1
6	160,491	12	82,171,392	6,144	40,107	3
7	164,671	12	84,311,552	6,144	41,152	3
8	165,475	28	84,723,200	14,336	41,353	7



## The Output Tab

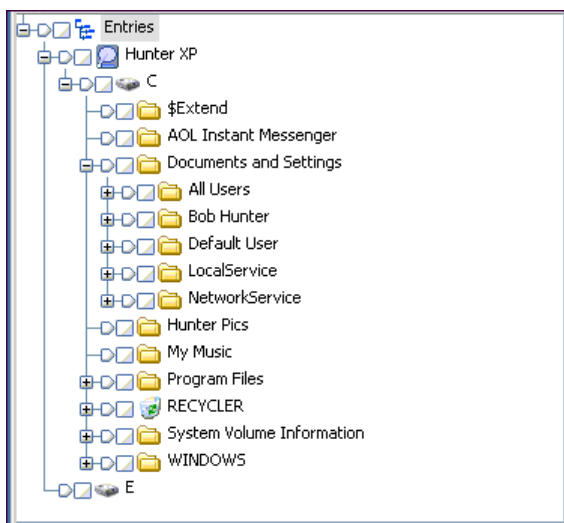
Use the Output tab to obtain output from various EnScript® programs.



## Navigating the Tree Pane

The Tree pane presents a structured view of all gathered evidence in a Windows-like folder hierarchy.

Use the structured view when exploring Entries, Bookmarks, Search Hits, Keywords, and other views of evidence. You can add folders to the structure to suit your working requirements. Note that some folders have a plus sign (+) next to them. Clicking the plus sign opens the folder and displays its contents.



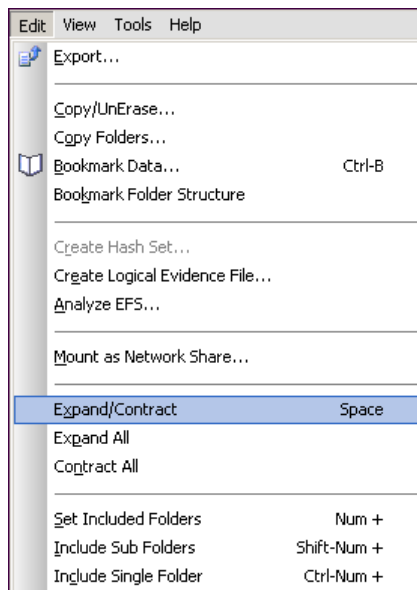
In the figure above, the Documents and Settings folder is expanded to show the five folders it contains. Note that the symbol next to the open folder is a - sign, indicating the folder is expanded.

## Opening and Closing Folders with Expand/Contract

Use the Edit menu or right-click in the Tree pane to use Expand/Contract to open or close the hierarchy at the point of the highlighted item.

To open and close all folders displayed in the Tree pane, do one of the following:

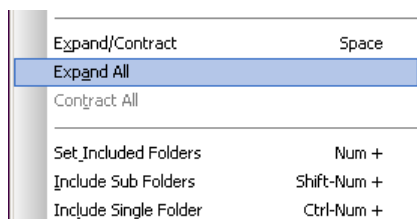
- Right-click the folder and choose Expand/Contract from the right-click menu.
- Click the Expand/Contract icon (+ or -).
- With the folder highlighted, press the space bar.



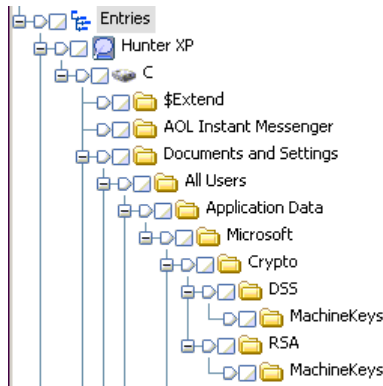
## Expand All

You can expand all nested folders beneath the highlighted folder with one menu click.

If the entire Tree pane hierarchy is closed, or if one or more folders are open, the entire tree can be expanded to display all of the contents.



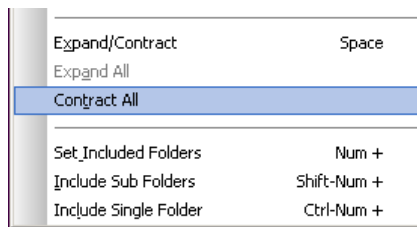
Use the right-click **Expand All** command to show all of the hierarchy. Start at the Entries root to open all available folders.



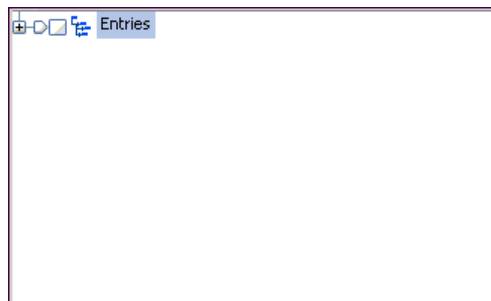
## Contract All

You can close an entire tree with one menu click. If one or more folders is expanded beneath the highlighted item, the entire tree is contracted.

Contract the entire table by opening the Edit Menu, then click **Contract All**.



The hierarchical tree contracts and displays the highlighted item only.

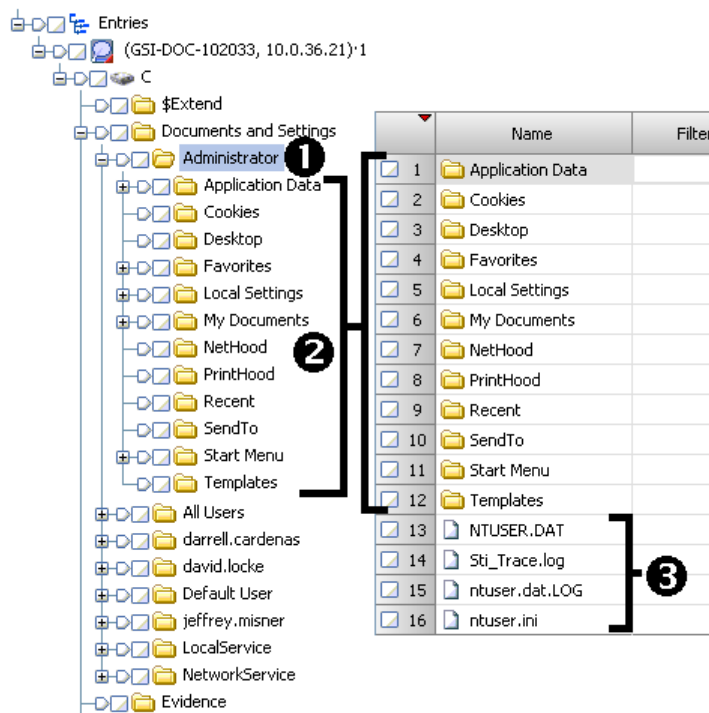


## Displaying Tree Entry Information for One Branch

Highlighting is one of three ways to choose items in the Tree pane.

Highlighting an item in the tree displays its contents in the Table pane.

*Figure 22 Highlighting a tree entry, where 1) is the highlighted item 2) are folder objects contained in the highlighted item in the Tree pane ,and 3) are items contained in the highlighted item, enumerated in the Table pane.*



Highlighting differs from selecting. Selecting--clicking one or more check boxes--constructs a collection for processing by an analytic operation such as bookmarking or hashing.

Highlighting also differs from including. Including--clicking to display the green polygon--displays all the items found in the included branch of the tree from the top level, down to the item you clicked.

## Displaying Expanded Tree Entry Information

You can include all the lower levels of the hierarchy of an item for display in the Table tab with a single mouse click.

You do not have to explicitly expand the tree folders. When you click the **Set Include** polygon in the Tree pane, or right- click and choose **Set Include** from the menu, this occurs:

- The **Set Include** icon of the highlighted item turns green.
- Items on the lower levels of the hierarchy are also included, as indicated by the green icons.
- The content of all the entries or objects included appear in the Table pane.

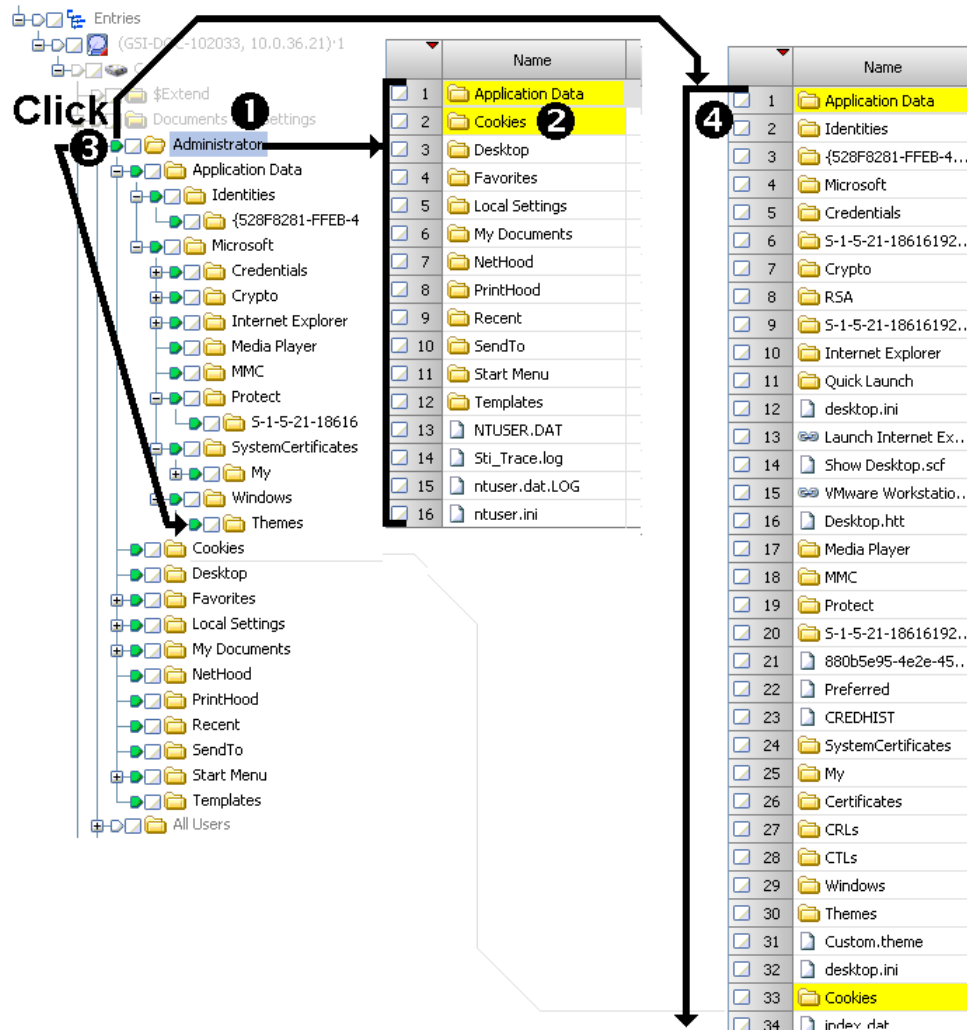
If the Include All icon is not green, the data associated with that item does not appear in the Table pane.

Including All is distinct from highlighting in that Including All displays all the items in the branch from the selected entry to the leaf entries, while highlighting displays only items contained in the highlighted item

In the Tree pane, including all is distinct from selecting because including all affects the contents of the table pane, while selecting does not.

Initially, **Set Include** displays the entries and objects in the Table pane in a hierarchical order. Sorting columns in the table destroys this order, which cannot be recovered except to cycle the **Set Include**. Use the status line to see the parent for a particular entry in the table.

Figure 23 Comparing Highlighting and Set Include, where the contents of 1) the highlighted entry in the Tree pane ,as 2) it appears in the Table pane, and where the content of the 3) **Set Include** entry that enables the rest of the Set Include entries in the subtree, as 4) it displays in the Table pane. Include propagates down the tree from 3) ,the entry initially included to the parallel entries.



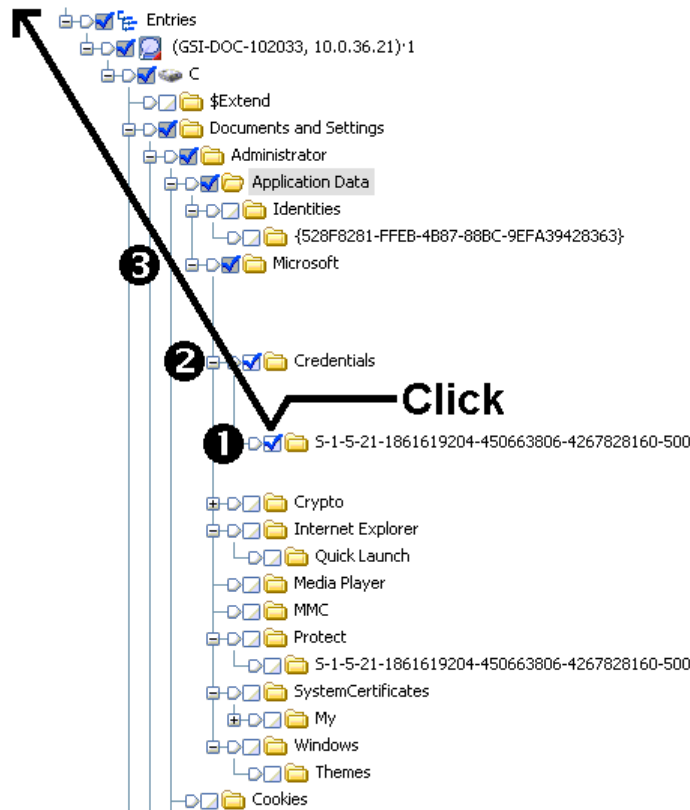
## Selecting Tree Entries for Operations

Selection is the way to choose multiple items in the Tree pane to manage them.

While highlighting and including in the Tree pane drive the content of the Table pane, selecting does not. Selecting determines which entries are processed by analytic operations such as bookmarking, searching, filtering, and hashing.

When you select an item by clicking a check-box, the selection propagates upwards in the hierarchy to include related structure.

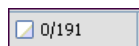
Figure 24 Selecting items where 1) is the item that you checked with a mouse click, 2) is a selected ancestor that was propagated from the initial selection, whose entire contents are included in a future operation, as indicated by the white background of the checkbox, and 3) is a selected ancestor, that was propagated from the initial selection, whose contents are not included; as a result, its checkbox has a gray background. The arrow shows the direction of the propagation.



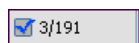
## Using the Dixon Box

The Dixon Box is located in the tab above the Report pane and shows how many files are selected and how many files exist in the case.

If no files are selected in the open case, the box looks like this:



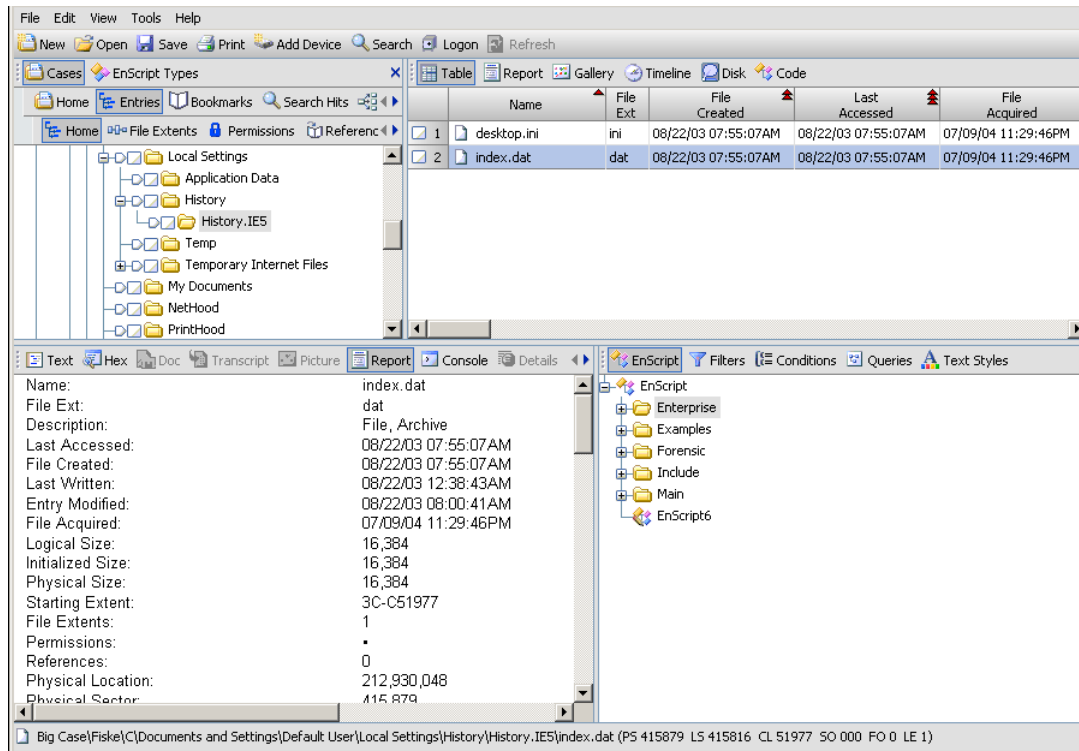
In this picture, three of the same 191 files are selected:



Note: To quickly select or deselect all files in a case, click the Dixon Box.

## Modifying the Table Pane

The Table pane displays the contents of selected files and folders.



Note: Contents of the Table pane change as different items are selected in Tree pane and when files are clicked in the Table pane.

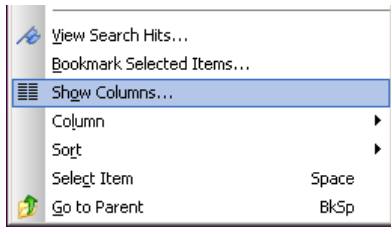


## Showing Columns

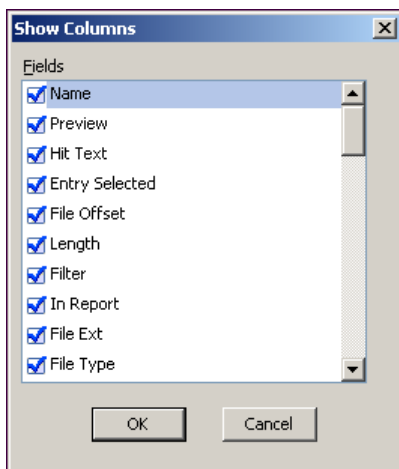
Individual or groups of columns can be shown and hidden from view.

To show or hide columns using the Show Columns, place the cursor in the Table pane and right-click. This menu option appears below.

To activate or deactivate the Table columns dialog right-click the Table pane, select Show Columns and select the desired columns.



The Show Columns dialog looks like this:



---

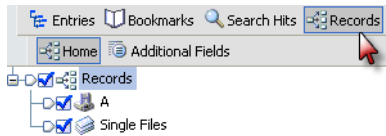
Note: See **Table Tab Columns** (on page 102) for information on all columns.

---

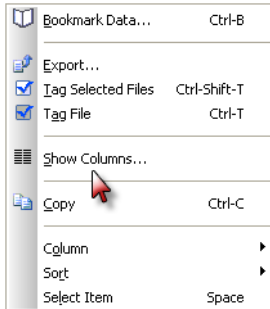
To hide columns, clear the appropriate check boxes, then click **OK**.

## Showing Columns in the Records Tab

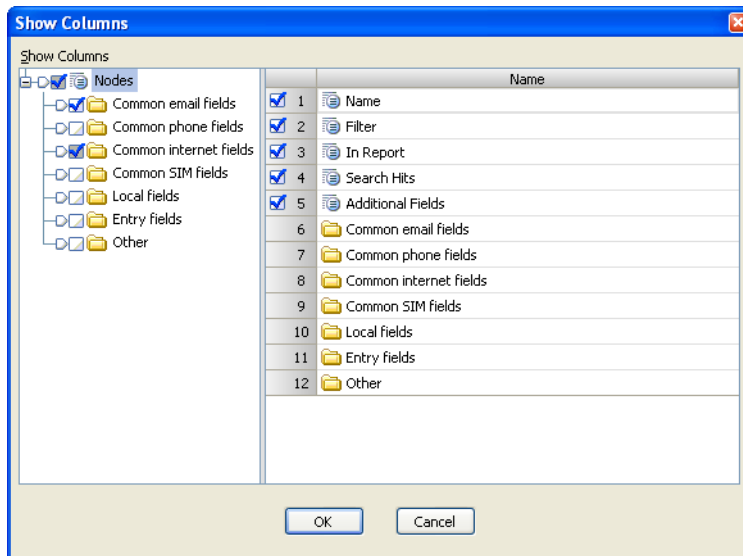
1. Select the Records Tab.



2. Right-click in the blank area of the Table pane and select **Show Columns**.

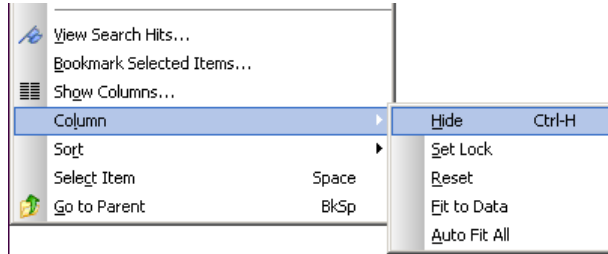


3. The columns display in a tree structure:



## Hiding Columns

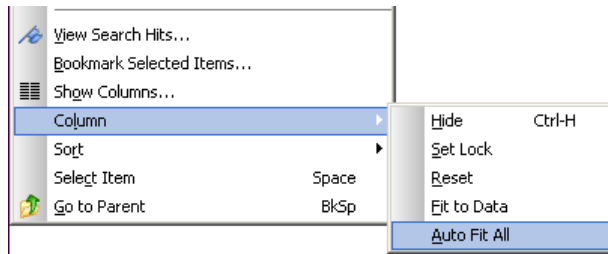
You can hide individual columns. Right-click the column you want to hide and click **Hide**.



The column in which the cursor was located is hidden.

## Auto Fit All Columns

The Auto Fit All feature expands the width of each column so no data are hidden.



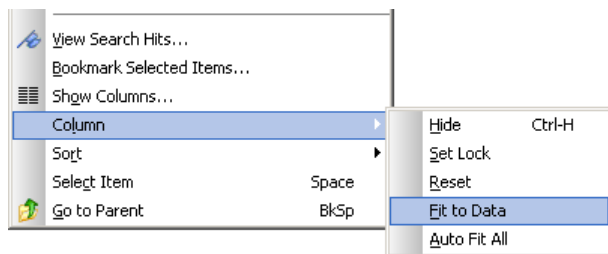

---

**Note:** The difference between Auto Fit All and Fit to Data is that with Auto Fit All, each displayed column is expanded to show its entire contents.

---

## Fitting Columns to Data

At times, you may want to adjust the width of only one column. To view the entire column, select Fit to Data.




---

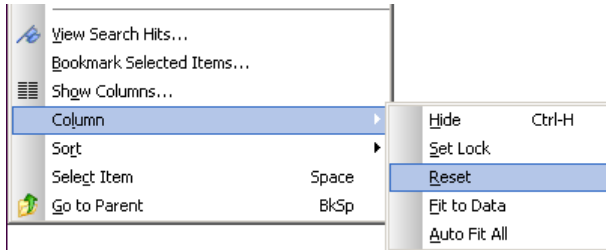
**Note:** If a column contains too much data, widen the column by clicking Fit to Data in the Column sub-menu.

---

## Resetting Columns

Restore columns to their default order and width by using reset.

Manually resize a column by dragging the column separator.



You can change the order in which the columns appear by grabbing the column header and dragging the column to the desired location.

---

Note: Change column order by left-clicking the column header and dragging it to another location.

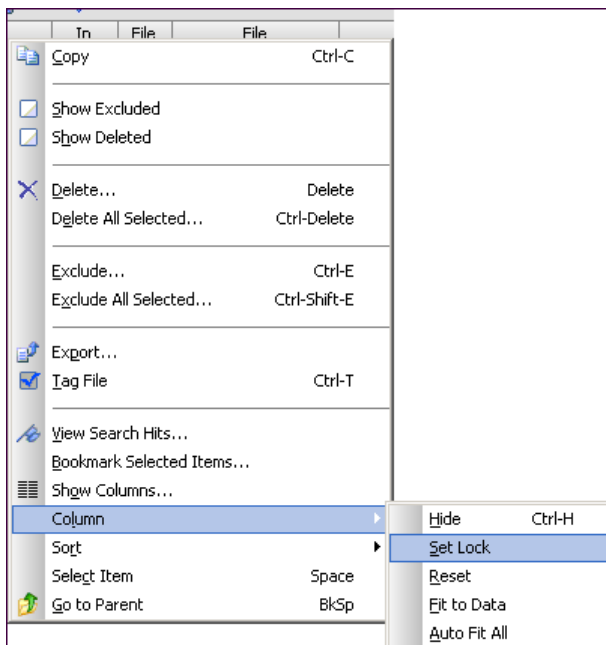
---

## Setting a Lock on Columns

Use Set Lock to scroll right and left in a table while continuing to show certain columns.

Columns are locked on the left side of the Table pane. To lock a column:

1. Place the cursor in a column to be locked.
2. Right-click and select **Set Lock** in the sub-menu.

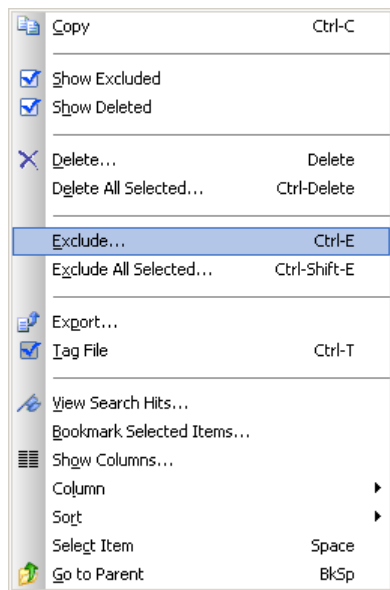


The lock is set on the position of the column. If other columns are moved into that position, they too are locked. To release the lock:

1. Right-click the locked column.
2. Select **Columns**.
3. Select **Unlock**.

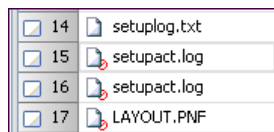
## Excluding Search Hits

The **Exclude** option hides one or more search hits from view. It does not delete them from the case.



Note: Excluded search hits are indicated by the international Not symbol.

In the figure below, the file `setuplog.txt` is included, while those in rows 15, 16, and 17 are excluded.



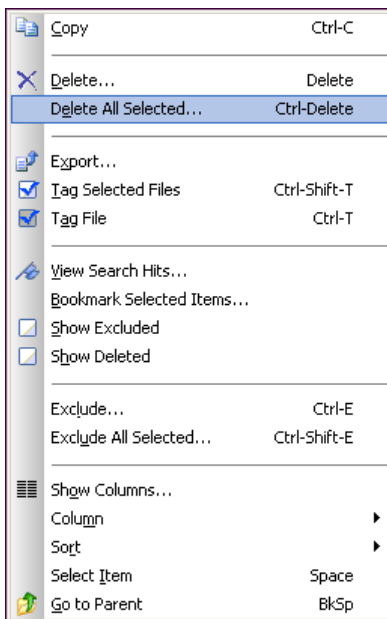
## Deleting Items

When using Search Hits, delete is considered a soft delete which you can undelete until the case is closed. If a search hit remains deleted when the case is closed, the hit is permanently deleted. In other tabs, however, undelete works only with the last selection deleted. Once a file is closed, deleted items are permanently removed and cannot be recovered.

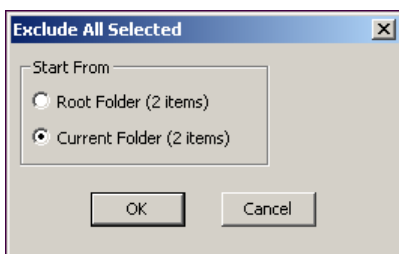
Run, then view a keyword search. This process is similar to the *Exclude Files* (on page 360) feature.

View the search hits report in the Table pane before excluding them from the report.

1. Select files to exclude, then right-click the view, selecting either **Delete** or **Delete All Selected**.



Selecting the latter displays the **Exclude All Selected** dialog.



2. Select the appropriate option and click **OK**. The selected files are temporarily deleted.

---

Note: Viewing the report shows the concatenated results.

---

# Filters

Filters are EnScripts that modify what data are displayed.

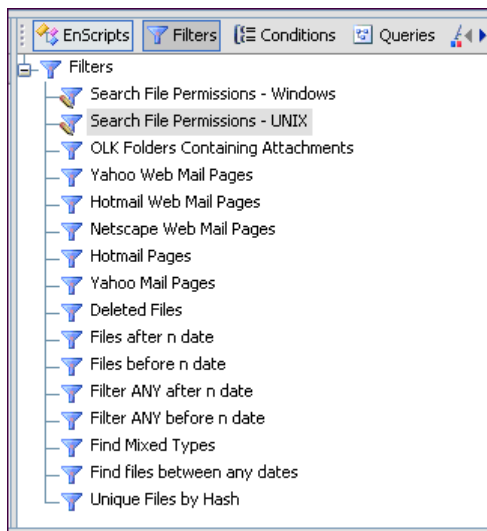
---

Note: There are different types of filters available depending on the tab chosen on the Tree pane. For example, the filters available for search hits are different from those available for entries.

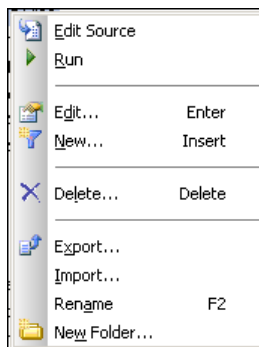
---

Several filters exist for filtering out objects of little or no interest to an investigation. Filters do not remove these objects from the case, they simply hide them from the Table pane.

The Filter pane allows investigators to run, create, edit, or delete filters, conditions, and queries. The Conditions tab allows the user to build filters by simply specifying parameters.



Right-click on a filter to open a sub-menu.



Use **New** to create filters based on set conditions that are menu-selectable.

Created filters reside in an initialization file (C:\Program Files\EnCase6\Config\filters.ini ). Filters are saved globally within the EnCase program.

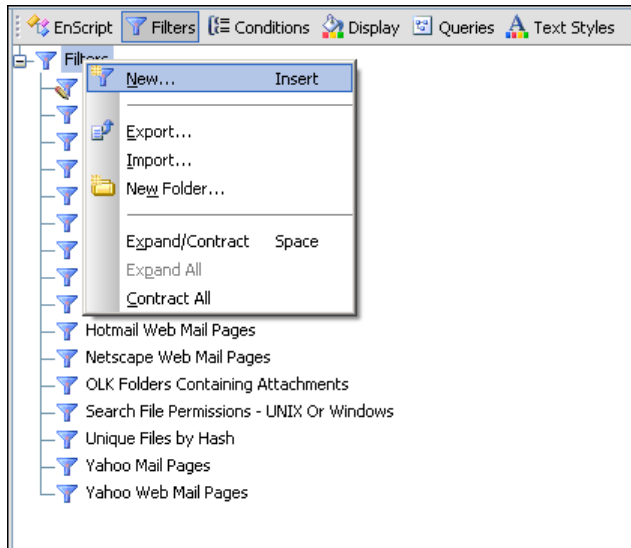
## Creating a Filter

New filters of your own creation can be added to the list.

Display the Filter list in the **Filter** pane, then create a new filter.

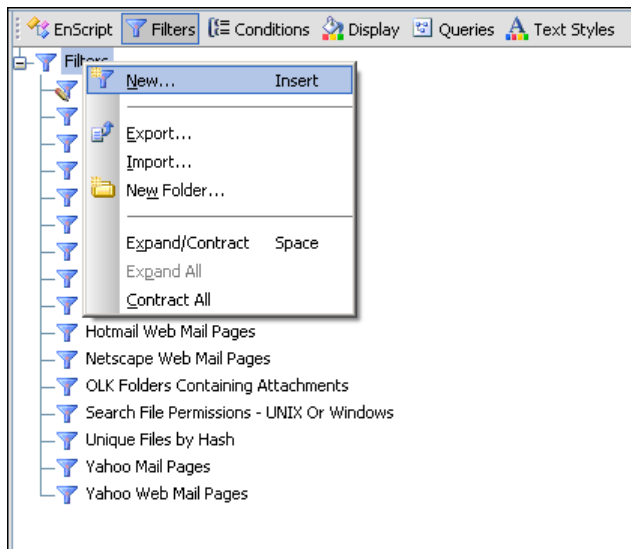
1. Right-click topmost **Filter** icon.

A sub-menu appears.



2. Click **New** from the drop down menu.

The New Filter dialog appears.





3. Enter a descriptive name in the **Filter Name** field and click **OK**.

A source editor appears in the **Table** pane.

```
class MainClass {
    bool Main(EntryClass entry) {
        return true;
    }
}
```

4. Enter EnScript code as required to accomplish your task.

The newly created filter name appears at the bottom of the **Filter** pane list.

Execute the new filter as required by double clicking it.

## Editing a Filter

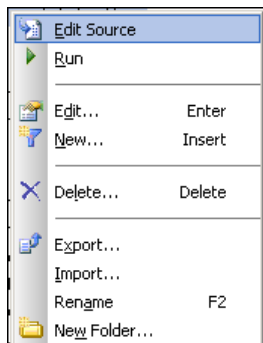
Change a filter's behavior by editing it.

Display the Filter list in the **Filter** pane, then edit it.

Edit a filter as follows:

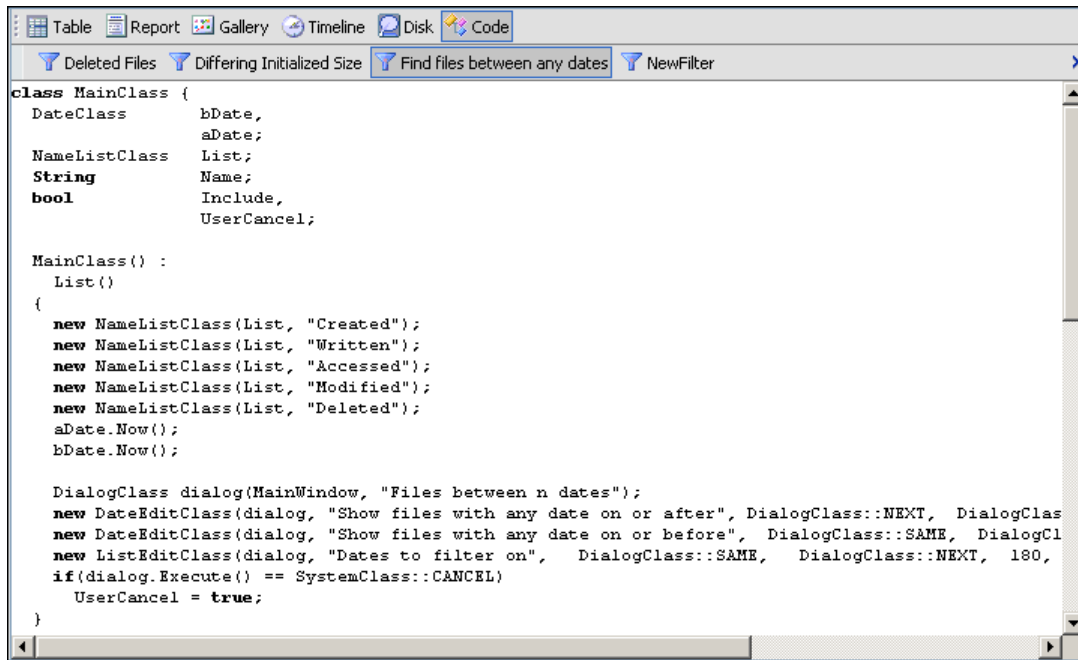
1. Right-click the filter you want to edit.

A drop-down menu appears.



2. Click **Edit Source**.

The filter source appears in the **Table** pane.



Note: The **Table** pane menu shows the Code icon selected, the text editor's menu highlights the filter you are editing, and the scroll bars allow you to maneuver in the display.

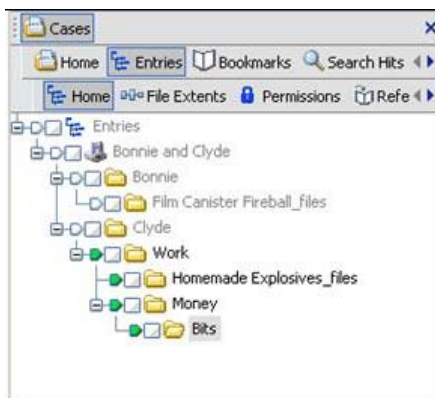
3. Edit commands as needed. Filter behavior changes.

## Running a Filter

Running a filter against a set of evidence files produces data that conform to the filters parameters.

Open a case file and select folders to search.

1. Run a filter by clicking Select All (home plate) on evidence folders. The **Tree** pane that appears is similar to this illustration.



2. Double-click a filter, or right-click it and select **Run** from the drop-down menu that appears. Complete any dialogs that appear.

When the filter finishes, the **Table** pane displays entries that meet the filter's criteria. The figure below shows the filter name and other data on those files that meet the requirements (**Deleted Files** in this case).

Query					
Table Report Gallery Timeline Disk Code					
	Name	Filter	Is Deleted	Last Written	File Created
<input checked="" type="checkbox"/>	1 _ORTRAIT.JPG	Deleted Files	Yes	04/30/00 04:19:38PM	01/28/05 08:05:08AM
<input checked="" type="checkbox"/>	2 _KSHIFT.JPG	Deleted Files	Yes	04/30/00 04:19:46PM	01/28/05 08:05:02AM
<input checked="" type="checkbox"/>	3 microprinting.jpg	Deleted Files	Yes	04/30/00 04:19:48PM	01/28/05 08:04:58AM
<input checked="" type="checkbox"/>	4 _UMBERS.JPG	Deleted Files	Yes	04/30/00 04:19:54PM	01/28/05 08:05:04AM
<input checked="" type="checkbox"/>	5 linesmoire.jpg	Deleted Files	Yes	04/30/00 04:19:56PM	01/28/05 08:04:52AM
<input checked="" type="checkbox"/>	6 _EAL.JPG	Deleted Files	Yes	04/30/00 04:20:00PM	01/28/05 08:05:24AM
<input checked="" type="checkbox"/>	7 fedreserveandrea...	Deleted Files	Yes	01/06/01 11:49:58PM	01/28/05 08:04:46AM
<input checked="" type="checkbox"/>	8 portrait1.jpg	Deleted Files	Yes	01/06/01 11:49:58PM	01/28/05 08:05:10AM
<input checked="" type="checkbox"/>	9 fedreserveandrea...	Deleted Files	Yes	01/06/01 11:49:58PM	01/28/05 08:04:48AM
<input checked="" type="checkbox"/>	10 _ORDER.JPG	Deleted Files	Yes	01/06/01 11:50:04PM	01/28/05 08:04:42AM
<input checked="" type="checkbox"/>	11 serialnumbers.jpg	Deleted Files	Yes	01/06/01 11:50:04PM	01/28/05 08:05:28AM
<input checked="" type="checkbox"/>	12 raisednoteten.jpg	Deleted Files	Yes	01/07/01 12:01:00AM	01/28/05 08:05:14AM
<input checked="" type="checkbox"/>	13 Counterfeit_finepri...	Deleted Files	Yes	01/07/01 12:06:08AM	01/28/05 08:04:44AM
<input checked="" type="checkbox"/>	14 Mellon.GIF	Deleted Files	Yes	01/07/01 12:11:58AM	01/28/05 08:04:56AM
<input checked="" type="checkbox"/>	15 _EAL-1.GIF	Deleted Files	Yes	01/07/01 12:12:00AM	01/28/05 08:05:18AM
<input checked="" type="checkbox"/>	16 _EAL-2.GIF	Deleted Files	Yes	01/07/01 12:12:10AM	01/28/05 08:05:20AM
<input checked="" type="checkbox"/>	17 _TRONG.GIF	Deleted Files	Yes	01/07/01 12:12:16AM	01/28/05 08:05:32AM
<input checked="" type="checkbox"/>	18 _RANK2.JPG	Deleted Files	Yes	01/07/01 12:25:06AM	01/28/05 08:04:50AM

3. Notice that a **Query** icon (below) appears in the top menu bar. This icon appears when a filtered list is displayed.

Clicking the icon changes the display from showing the filtered list to showing all file entries.



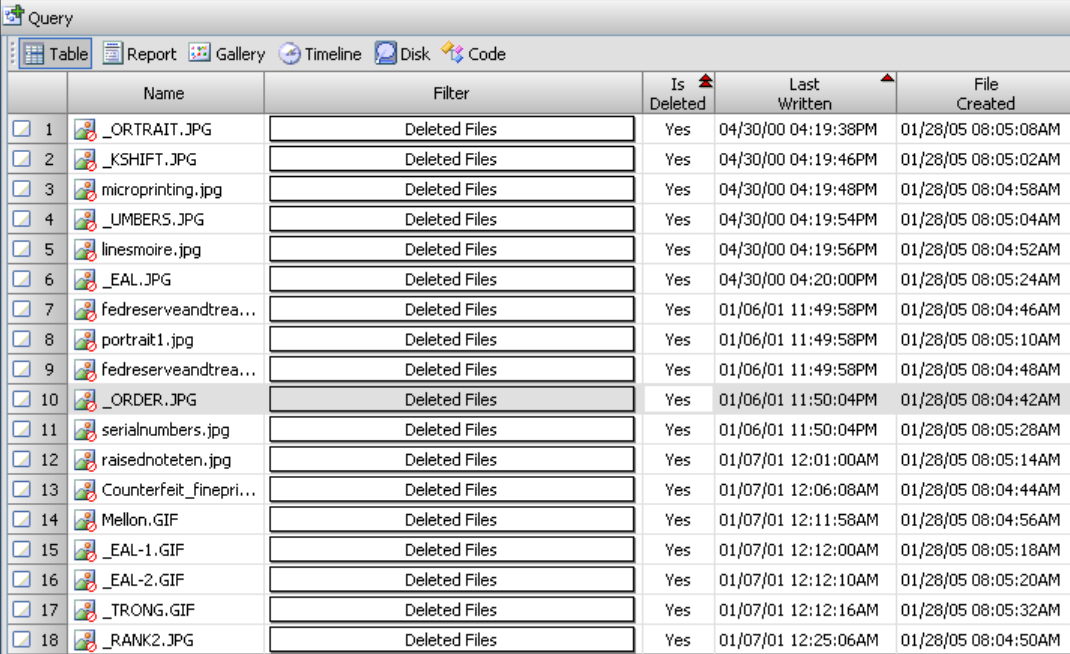
The Query icon changes when clicked. It has a red - sign on it to show the filter is off. This does not delete the filter; it only turns its display effects off.



## Combining Filters

You can run multiple filters, and combine filters with **Conditions** and **Queries**.

To do this, run more than one filter. Running multiple filters uses **OR** logic to select files, thus the shows both deleted and selected files. Any entry that responds to any active filter condition or query appears. The first figure shows a filtered list with one filter run against it.

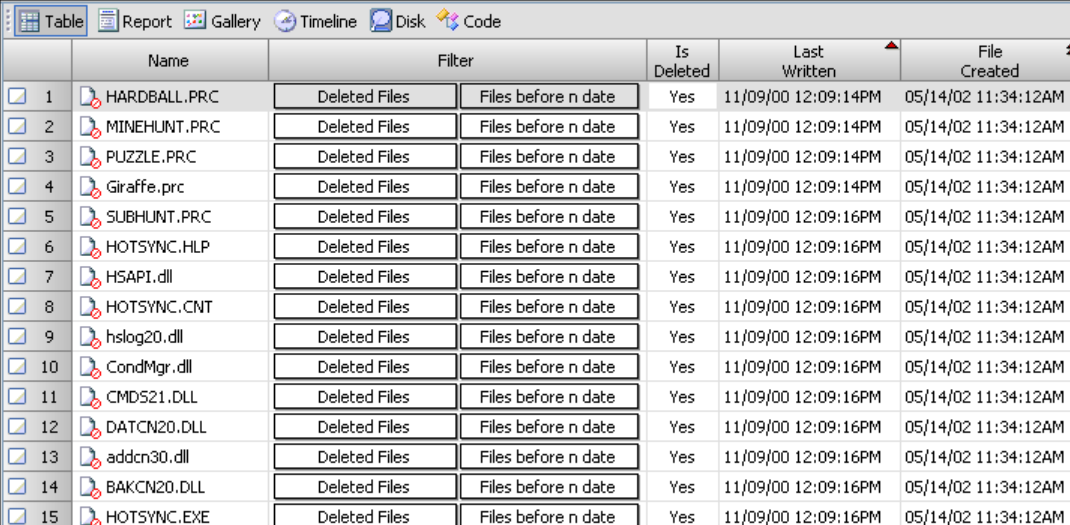


The screenshot shows the 'Query' window in EnCase Forensic. The 'Table' tab is selected, displaying a list of 18 files. Each file has a checkbox, a thumbnail icon, a name, a filter applied, and columns for 'Is Deleted', 'Last Written', and 'File Created'. All files are marked as 'Deleted'.

	Name	Filter	Is Deleted	Last Written	File Created
<input checked="" type="checkbox"/>	1 _ORTRAIT.JPG	Deleted Files	Yes	04/30/00 04:19:38PM	01/28/05 08:05:08AM
<input checked="" type="checkbox"/>	2 _KSHIFT.JPG	Deleted Files	Yes	04/30/00 04:19:46PM	01/28/05 08:05:02AM
<input checked="" type="checkbox"/>	3 microprinting.jpg	Deleted Files	Yes	04/30/00 04:19:48PM	01/28/05 08:04:58AM
<input checked="" type="checkbox"/>	4 _UMBERS.JPG	Deleted Files	Yes	04/30/00 04:19:54PM	01/28/05 08:05:04AM
<input checked="" type="checkbox"/>	5 linesmoire.jpg	Deleted Files	Yes	04/30/00 04:19:56PM	01/28/05 08:04:52AM
<input checked="" type="checkbox"/>	6 _EAL.JPG	Deleted Files	Yes	04/30/00 04:20:00PM	01/28/05 08:05:24AM
<input checked="" type="checkbox"/>	7 fedreserveandrea...	Deleted Files	Yes	01/06/01 11:49:58PM	01/28/05 08:04:46AM
<input checked="" type="checkbox"/>	8 portrait1.jpg	Deleted Files	Yes	01/06/01 11:49:58PM	01/28/05 08:05:10AM
<input checked="" type="checkbox"/>	9 fedreserveandrea...	Deleted Files	Yes	01/06/01 11:49:58PM	01/28/05 08:04:48AM
<input checked="" type="checkbox"/>	10 _ORDER.JPG	Deleted Files	Yes	01/06/01 11:50:04PM	01/28/05 08:04:42AM
<input checked="" type="checkbox"/>	11 serialnumbers.jpg	Deleted Files	Yes	01/06/01 11:50:04PM	01/28/05 08:05:28AM
<input checked="" type="checkbox"/>	12 raisednoteten.jpg	Deleted Files	Yes	01/07/01 12:01:00AM	01/28/05 08:05:14AM
<input checked="" type="checkbox"/>	13 Counterfeit_finepri...	Deleted Files	Yes	01/07/01 12:06:08AM	01/28/05 08:04:44AM
<input checked="" type="checkbox"/>	14 Mellon.GIF	Deleted Files	Yes	01/07/01 12:11:58AM	01/28/05 08:04:56AM
<input checked="" type="checkbox"/>	15 _EAL-1.GIF	Deleted Files	Yes	01/07/01 12:12:00AM	01/28/05 08:05:18AM
<input checked="" type="checkbox"/>	16 _EAL-2.GIF	Deleted Files	Yes	01/07/01 12:12:10AM	01/28/05 08:05:20AM
<input checked="" type="checkbox"/>	17 _TRONG.GIF	Deleted Files	Yes	01/07/01 12:12:16AM	01/28/05 08:05:32AM
<input checked="" type="checkbox"/>	18 _RANK2.JPG	Deleted Files	Yes	01/07/01 12:25:06AM	01/28/05 08:04:50AM

Note that the entry in the **Is Deleted** column is marked **True**.

This second figure shows the display that results when two filters, **Deleted Files** and **Files Before n**, are run. The names of both filters appear in the **Filter** column of the **Table** pane.



The screenshot shows the 'Query' window in EnCase Forensic. The 'Table' tab is selected, displaying a list of 15 files. Each file has a checkbox, a thumbnail icon, a name, and two filters applied: 'Deleted Files' and 'Files before n date'. The columns for 'Is Deleted', 'Last Written', and 'File Created' are also visible.

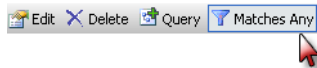
	Name	Filter	Is Deleted	Last Written	File Created
<input checked="" type="checkbox"/>	1 HARDBALL.PRC	Deleted Files Files before n date	Yes	11/09/00 12:09:14PM	05/14/02 11:34:12AM
<input checked="" type="checkbox"/>	2 MINEHUNT.PRC	Deleted Files Files before n date	Yes	11/09/00 12:09:14PM	05/14/02 11:34:12AM
<input checked="" type="checkbox"/>	3 PUZZLE.PRC	Deleted Files Files before n date	Yes	11/09/00 12:09:14PM	05/14/02 11:34:12AM
<input checked="" type="checkbox"/>	4 Giraffe.prc	Deleted Files Files before n date	Yes	11/09/00 12:09:14PM	05/14/02 11:34:12AM
<input checked="" type="checkbox"/>	5 SUBHUNT.PRC	Deleted Files Files before n date	Yes	11/09/00 12:09:16PM	05/14/02 11:34:12AM
<input checked="" type="checkbox"/>	6 HOTSYNC.HLP	Deleted Files Files before n date	Yes	11/09/00 12:09:16PM	05/14/02 11:34:12AM
<input checked="" type="checkbox"/>	7 HSAPI.dll	Deleted Files Files before n date	Yes	11/09/00 12:09:16PM	05/14/02 11:34:12AM
<input checked="" type="checkbox"/>	8 HOTSYNC.CNT	Deleted Files Files before n date	Yes	11/09/00 12:09:16PM	05/14/02 11:34:12AM
<input checked="" type="checkbox"/>	9 hslg20.dll	Deleted Files Files before n date	Yes	11/09/00 12:09:16PM	05/14/02 11:34:12AM
<input checked="" type="checkbox"/>	10 CondMgr.dll	Deleted Files Files before n date	Yes	11/09/00 12:09:16PM	05/14/02 11:34:12AM
<input checked="" type="checkbox"/>	11 CMD521.DLL	Deleted Files Files before n date	Yes	11/09/00 12:09:16PM	05/14/02 11:34:12AM
<input checked="" type="checkbox"/>	12 DATCN20.DLL	Deleted Files Files before n date	Yes	11/09/00 12:09:16PM	05/14/02 11:34:12AM
<input checked="" type="checkbox"/>	13 addcn30.dll	Deleted Files Files before n date	Yes	11/09/00 12:09:16PM	05/14/02 11:34:12AM
<input checked="" type="checkbox"/>	14 BAKCN20.DLL	Deleted Files Files before n date	Yes	11/09/00 12:09:16PM	05/14/02 11:34:12AM
<input checked="" type="checkbox"/>	15 HOTSYNC.EXE	Deleted Files Files before n date	Yes	11/09/00 12:09:16PM	05/14/02 11:34:12AM

A similar result would occur if you were to combine a filter and a condition.

## AND/OR Filter Logic

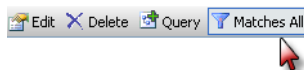
You can toggle between displaying only entries that match all the active filters (AND functional logic) or entries matching any of the active filters (OR functional logic).

When you run multiple filters, a **Matches Any** option displays in the toolbar:



This option employs OR logic to display files.

To employ AND logic, click the **Matches Any** toolbar option. The option changes to **Matches All**:

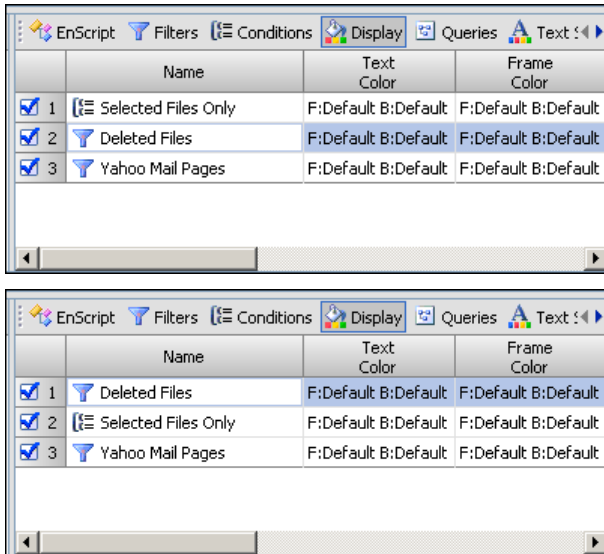


## Changing Filter Order

Filters run in the order in which you selected them. To change this order:

1. Click **Display** to show the active filters.
2. Left-click the filter you want to move.
3. While holding the left mouse button down, move the selected filter to a new position.

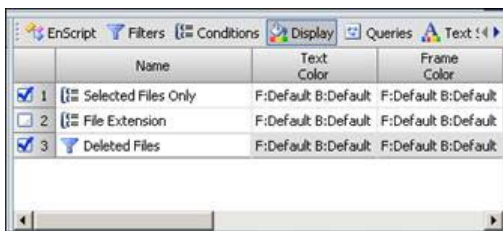
A three-filter list with all items selected is shown below. The next example shows the same three filters in a new order. Because all filters are selected, and thus active, all will be run. The order in which they run, however, is changed. In the first example below, Selected Files Only runs first, while in the second example, it runs second.



## Turning Filters Off

There are several ways to turn off or disable filters. You can toggle the Query icon to alternate between the filtered list and the unfiltered one. This is an "all or none" toggle.

When you have more than one filter or condition in the Filters pane Display tab, deselecting a filter modifies the Table view to show only files that result from the still-checked items. For example, the list in the next example shows three active filters, Selected Files Only, File Extension and Deleted Files, but File Extension is unchecked.



## Deleting a Filter

You can remove a filter from the Display list by selecting it, right-clicking it, and then clicking **Delete** from the drop down menu. As a safeguard, a dialog displays. Click **Yes** to complete the deletion. The Table pane display automatically updates to reflect the change. The filter, condition, or query is not deleted from the Filters, Conditions, or Queries tab from which it was executed.

## Importing Filters

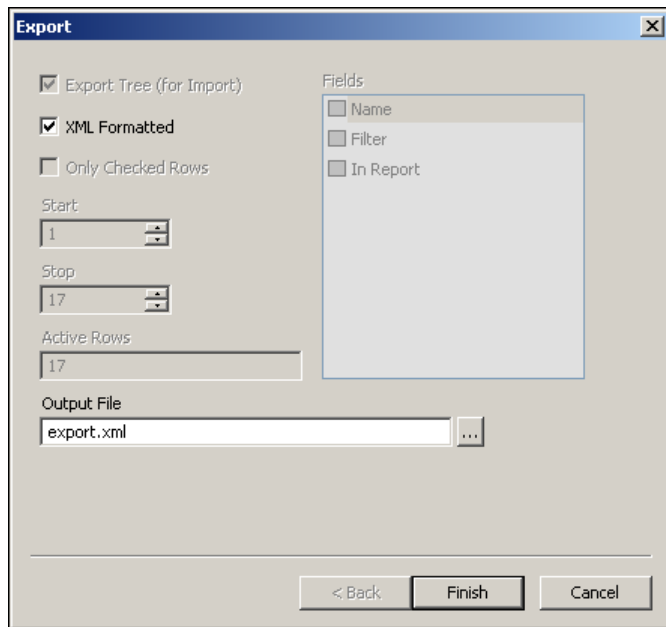
Filters others create can be imported into your collection and used.

*To import a filter someone else has written,*

1. Right-click in the Filter pane.
2. Select Import.
3. Navigate to or enter the path where the filter is located and click **OK**.

## Exporting Filters

Send your filters in a text file to others.



To export a filter from your collection,

1. Right-click in the Filter pane.
2. Select **Export**.

---

Note: Selecting XML Formatted exports filters in XML format.

---

3. Check the Export Tree field as in the figure.
4. Navigate to or enter the path where the filter is located and click **OK**.

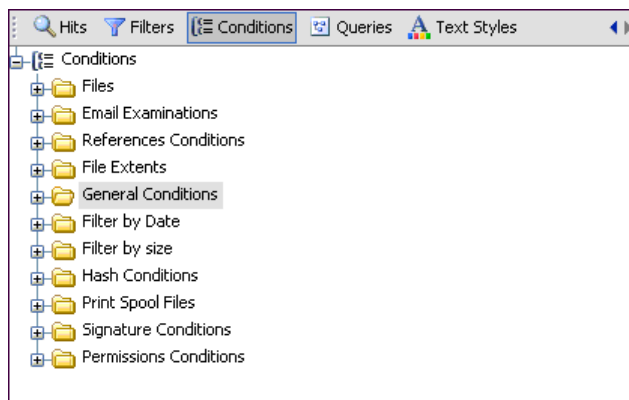
---

Note: By default, the Output File text field contains a file named export.txt. This can be changed and a complete export path can be entered or navigated to.

---

## Conditions

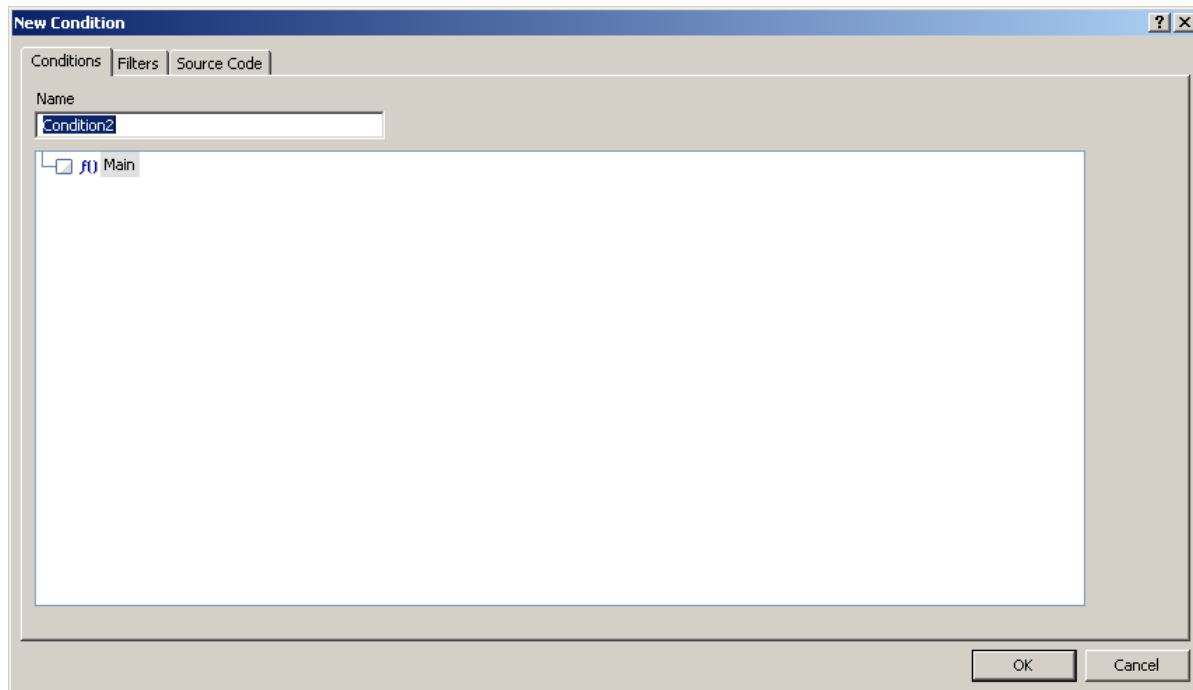
Conditions are similar to filters. They limit Table pane content. Several created conditions exist, and like filters, they vary depending on the chosen Tree tab. The first figure below shows the display when the Conditions tab is selected.





## Creating Conditions

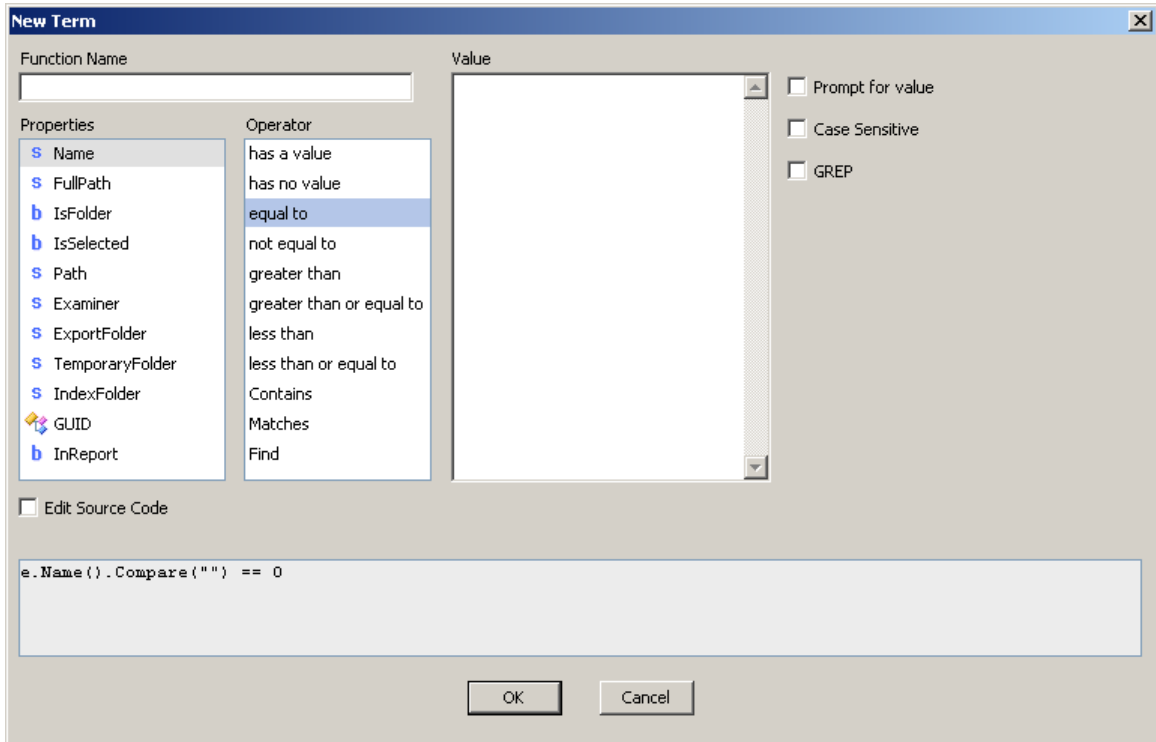
To create a new condition, right-click a folder in the Conditions tab in the Filter pane and select **New**.



Note: To use a filter inside a condition, create the filter by first clicking the filter tab and creating a filter. Once created, click the **Conditions** tab and the filter appears in the properties list.

*To create a condition:*

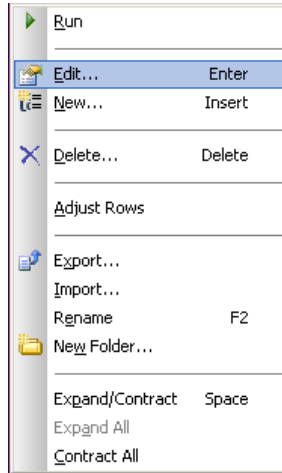
1. Enter a name in the **Name** field.
2. Right-click **Main** on the conditions tree and select **New** to see the New Term dialog.



3. Select a property, an operator, and, if prompted, a value and choice. Depending on the property and operator chosen, you can also select
  - ☐ **Prompt for Value**
  - ☐ **Case Sensitive**
  - ☐ **GREP**
4. To edit the source code, click **Edit Source Code**.
5. Repeat the steps above to create as many terms as you want to make the condition as detailed as possible.
6. Click **OK** to save the condition.
7. To nest terms, create a folder by right-clicking the desired location in the Tree pane and choosing **New Folder**. Place the nested terms inside this folder.
8. If you want to change the logic, right-click the term and select **Change Logic**. This changes the AND operator to an OR, and vice versa.
9. If you want to negate the logic, right-click the term and select **Not**.
10. When satisfied with the logic, click **OK**.

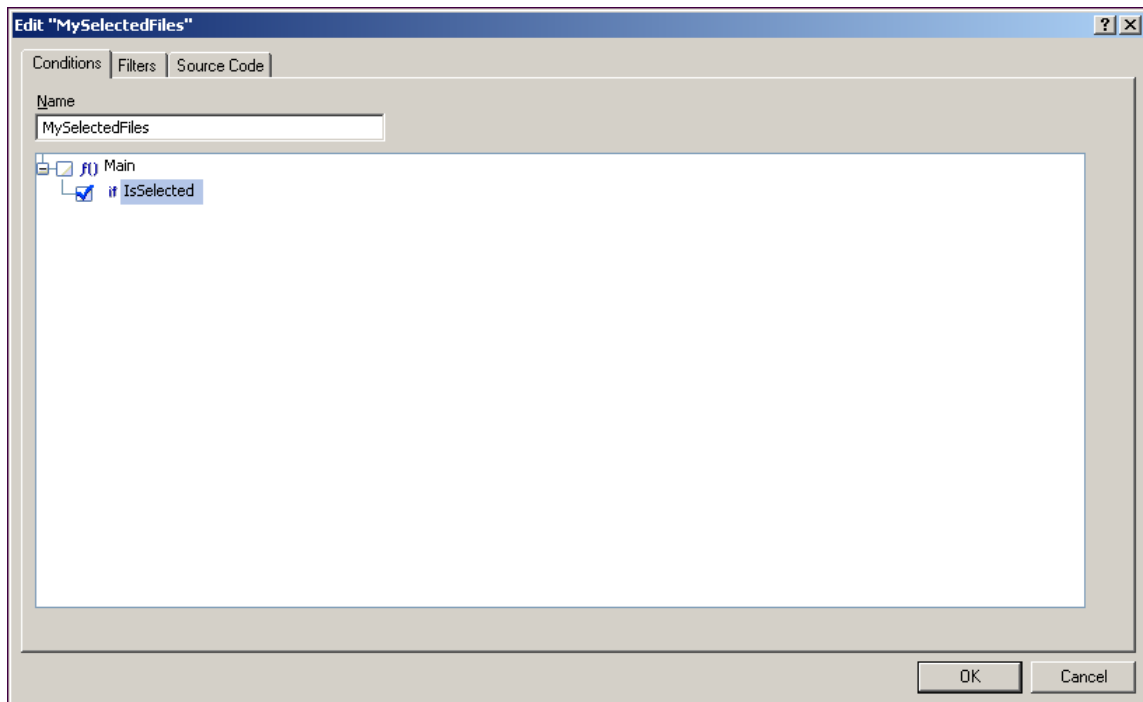
## Editing Conditions

Conditions can be opened and edited when there are no open cases.



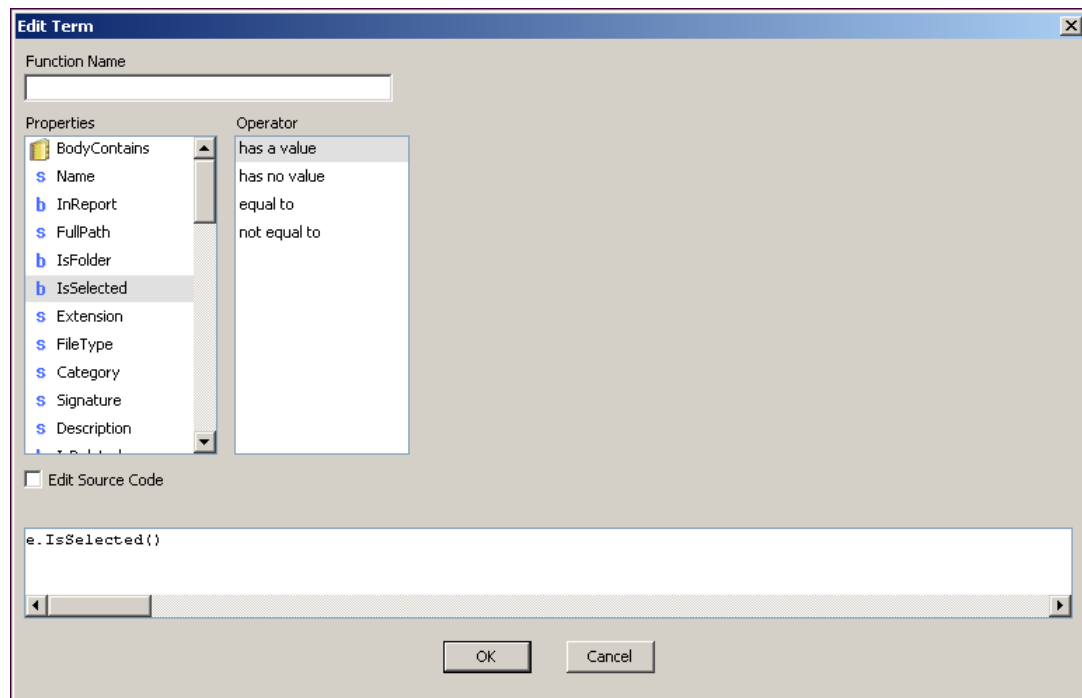
1. Select the filter.
2. Right-click it and select **Edit**.

The edit wizard opens in the Table pane.



3. Right-click the property and select **Edit** to see the Edit Term wizard.

4. Make the selected changes and click **OK**.



## Running Conditions

To run conditions, double click them, select an item and run the script against it, or right-click and select **Run**.

The example below shows the Table pane before a filter is run.

	Name	Filter
<input type="checkbox"/>	1 Application Data	
<input type="checkbox"/>	2 Microsoft	
<input type="checkbox"/>	3 Crypto	
<input type="checkbox"/>	4 DSS	
<input type="checkbox"/>	5 MachineKeys	
<input type="checkbox"/>	6 RSA	
<input checked="" type="checkbox"/>	7 MachineKeys	
<input type="checkbox"/>	8 Dr Watson	
<input type="checkbox"/>	9 drwtsn32.log	
<input checked="" type="checkbox"/>	10 user.dmp	
<input type="checkbox"/>	11 HTML Help	
<input type="checkbox"/>	12 hhcolreg.dat	
<input type="checkbox"/>	13 Media Index	
<input type="checkbox"/>	14 wmplibrary_v_0_12...	
<input type="checkbox"/>	15 Network	
<input type="checkbox"/>	16 Connections	
<input checked="" type="checkbox"/>	17 Pbk	
<input type="checkbox"/>	18 sharedaccess.ini	

Three rows are selected; 7, 10, and 17. Note the blank Filter column.

Running a condition changes the display several ways. First, the top tab menu displays the condition name and display tabs. Notice the + sign on both icons in the figure below.



The second change is that files to which the filter applies appear in the Condition column. In this case, we ran a filter looking for files that had any date before 21 September 2006. You can change the date and time in these files.

The Table view looks like this after the filter is run:

Table   Report   Gallery   Timeline   Disk   Code		
	Name	Filter
1	MachineKeys	MySelectedFiles
2	user.dmp	MySelectedFiles
3	Pbk	MySelectedFiles

Column numbers are changed, but the file selected names and the condition name appear as in the picture above.

To return to the original display, click the MySelectedFiles tab to change the + **sign** to a - **sign**.



All original files reappear with the filter in the field displayed on only those files which meet the parameters. To hide the filter name, select the Display tab and change it to a - **sign**.

## Importing Conditions

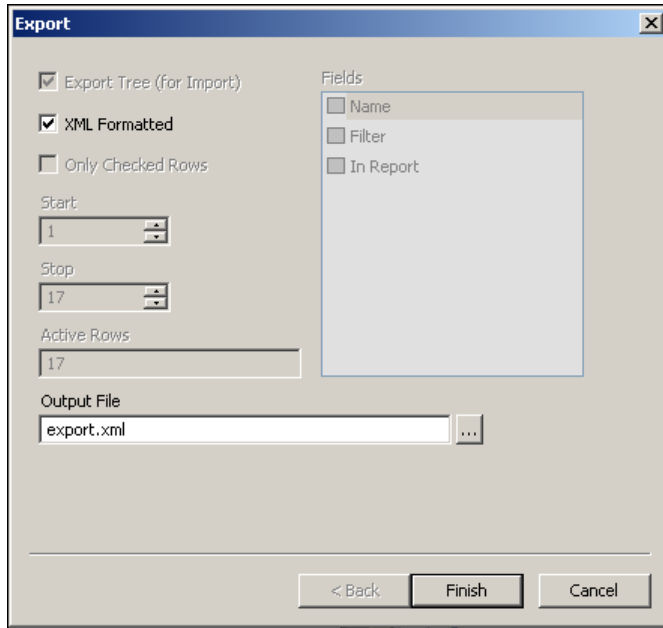
You can import conditions created by others.

To import a condition filter someone else has written:

1. Right-click in the Condition pane.
2. Select Import.
3. Navigate to or enter the path where the filter is located and click **OK**.

## Exporting Conditions

Export filters to share them with other users.



To export a filter from your collection:

1. Right-click in the Conditions pane.
2. Select **Export**.
3. Select **Export Tree**.

---

Note: Selecting XML Formatted exports the file in XML format.

---

4. Navigate to or enter the path where the filter is located and click **OK**.

---

Note: By default, the Output File text field contains a file named export.txt. You can change this name. You can also enter or browse to a complete export path.

---

## Queries

Queries allow changing what is visible by combining filters and conditions into one item. There are two parts to a query, the display portion and the logic portion. The display portion affects the text and its color, and is used to denote matches using user-selected filters and conditions. The logic portion actually controls which rows are hidden from the Table pane.

Construct a query using the same filters and conditions for the display and logic sections, or use different filters and conditions. One caveat: the logic portion takes precedence, so if a row is not a filters and conditions match used in the logic section, it is hidden even if it may have been a match in the display logic. The logic portion actually controls which rows are hidden from the Table pane.

### *To create a query:*

1. Enter a name in the field.
2. In the Display settings for shown items pane, right-click in the right pane and select new.
  - ☐ Choose Filter or Condition.
  - ☐ Select the filter or condition from the list.
  - ☐ Enter text into the text field. This text will appear in the filter column of the Table pane when a file meets this criteria.
  - ☐ Change the color element by clicking **Text Color** or **Frame Color**, then double click **Background** and **Foreground** colors, then click **OK**.
3. Choose Filter or Condition.
4. Select the filter or condition from the list.
5. Enter text into the text field. This is text will appear in the filter column of the Table pane when a file meets this criteria.
6. Change the Color element by clicking Text color or Frame color, then double-click the **Background** and **Foreground** colors, then click **OK**.
7. In the New Display dialog, repeat Step 4 as often as required.

---

Note: The filters and conditions shown here will not hide rows that do not match the requirements of the selected filters. These selections simply adjust how the matches are indicated in the interface.

---

8. In the Conditions for showing items pane, right-click Combinations and select **New**.
9. In the New Combination dialog, select filter or condition, then select the filter or condition from the list and click **OK**.

---

Note: You do not need to enter the same filters or conditions here as entered in the display setting for shown items pane.

---

10. Repeat Step 7 as many times as needed.

---

Note: This is the logic for hiding rows. If, for example, an item matches a filter from the display settings for shown items pane, but it does not match the logic in the conditions for showing items pane, then the row will not be shown.

---

11. The default logic for the conditions is AND. To change this logic to OR, right-click **Combinations > Combinations Change Logic > Change Logic**.
12. Click **OK**.

---

Note: Other operations, including exporting and importing are the same as filters and conditions.

---

## Gallery Tab

The Gallery tab is a quick, easy way to view images stored on subject media. The extent of files shown in Gallery tab of the Table view is determined by the selection made in the Tree pane. For example, to view images of the entire case, set-include at the root of the Case tree.

In Gallery, you can bookmark images just like bookmarking them in the Table tab.

If signature analysis is not yet run, Gallery view displays files based on published file extension. For example, if a JPG file is changed to DLL, it does not appear in the Gallery until a signature analysis is run.

---

Note: Running a signature analysis is suggested before performing analysis in the gallery tab.

---

See the *Signature Analysis* (on page 327) section of this manual for more information.

## Viewing More Columns

View more pictures in Gallery by increasing the number of displayed columns:

1. Right-click anywhere in Gallery.
2. Select **More Columns**.

## Viewing Fewer Columns

View fewer pictures in Gallery by reducing the number of displayed columns:

1. Right-click anywhere in Gallery.
2. Select the **Fewer Columns** menu option.

The rightmost column is hidden.



## Viewing More Rows

View more pictures in Gallery by increasing the number of displayed rows:

1. Right-click in the Gallery tab.
2. Select **More Rows**.

## Viewing Fewer Rows

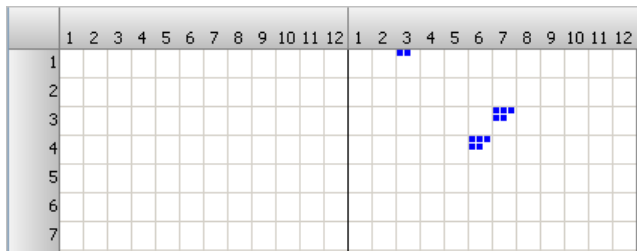
View fewer pictures in Gallery by decreasing the number of displayed rows:

1. Right-click anywhere in gallery.
2. Select **Fewer Rows**.

## Timeline Tab

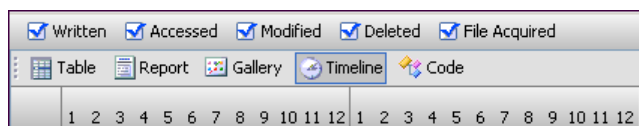
The Timeline is a great resource for looking at patterns of file creation, editing, and last accessed times.

You can zoom in to a second-by-second timeline and zoom out to a year-by-year timeline by right-clicking and selecting the appropriate option.



Above the calendar are selection boxes to quickly and easily filter which type of time stamp to display:

- ☒ Written
- ☒ Accessed
- ☒ Modified
- ☒ Deleted
- ☒ File Acquired



Clearing one or more of these boxes changes the timeline presentation.

## Modifying the View Pane

The View pane provides display-specific functionality of items selected in the Table pane.

### Copy

You can copy data in the Text and Hex tabs. You can also copy RTF from a report so it can be pasted into an external program that accepts RTF input.

In either tab, select the text, right-click and select **Copy**.

### Goto

Use Goto to specify where to move the cursor in the View pane.

To skip to a location:

1. Right-click in the View pane.
2. Select **Goto**.
3. Enter the file offset in the other field and click **OK**.

Goto can also interpret selected text using Little-Endian or Big-Endian. To interpret selected text:

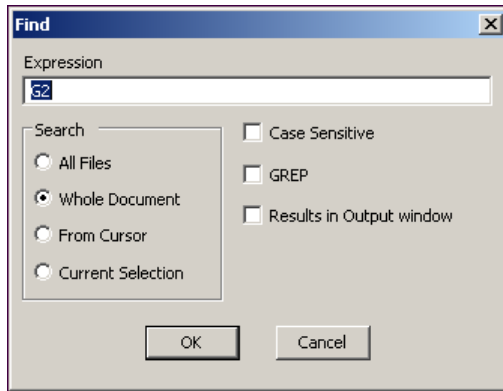
1. Highlight text in the View pane.
2. Right-click the View pane and choose **Goto**.
3. Click **Little- Endian** to see the representation in Little-Endian.
4. Click **Big- Endian** to see the representation in Big-Endian.

## Find

Find works in most tabs of the View pane. Use it to locate strings within data.

To find a string:

1. Display Text view.
2. Right-click the View pane.



3. Click **Find**.
4. Enter a string in the Expression field. To use a GREP expression, check the GREP option.
5. Select either Whole Document, From Cursor, or Current Selection.
6. Select Case Sensitive if desired.
7. Choose whether to have results appear in output pane.
8. Click **OK**.

The system finds the expression you entered.



# Case Management

- Overview of Case Structure 151
- Case Related Features 157
- New Case Wizard 166
- Using a Case 169
- Open a Case 175
- Saving a Case 176
- Close Case 177

## Overview of Case Structure

An evidence case has a tripartite structure consisting of an evidence file, a case file, and EnCase® program configuration files.

The case file contains information specific to one case. It contains

- pointers to one or more evidence files or previewed devices
- bookmarks
- search results
- sorts
- hash analysis results
- signature analysis reports

---

Note: A case file must be created before any media can be previewed or evidence files analyzed.

---

Indeed, one of the most powerful features of the program is its ability to organize different media so they can be searched as a unit rather than individually.

## Case Management

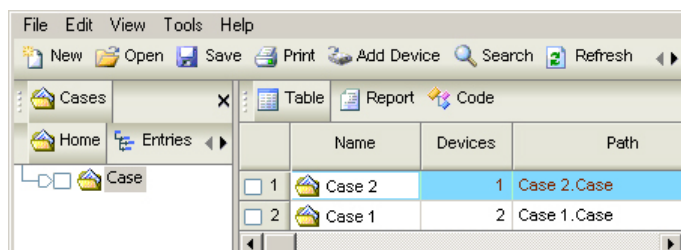
Before starting an investigation, give consideration to how the case is accessed once it is created. For example, more than one investigator may need to view the information. To accomplish this, evidence files can reside on a central server.

Creating temporary export and evidence folders allows file segregation and control. A temporary folder holds any transient files created during an investigation. The export folder provides a destination for data copied from the evidence file.

Create an evidence folder to store evidence. Temp and Export folders are built when a case is created.

## Concurrent Case Management

The program can open more than one case at a time. Each case appears in the Table pane, and is analyzed independent of the other.



*To switch case analysis from one case to another:*

1. Click **View > Cases Sub-Tabs > Home**.
2. Select a case for analysis from the Table tab.

The Devices column of the table indicates how many devices are associated with the case in the Name column.

---

Note: To look at the devices associated with a particular case, highlight the case in the Table pane, then click on the Entries sub-tab below Cases.

---

## Indexing a Case

Managing the index files associated with evidence files in a case is an important part of case management.

For detailed information, see *Indexing* (on page 365).

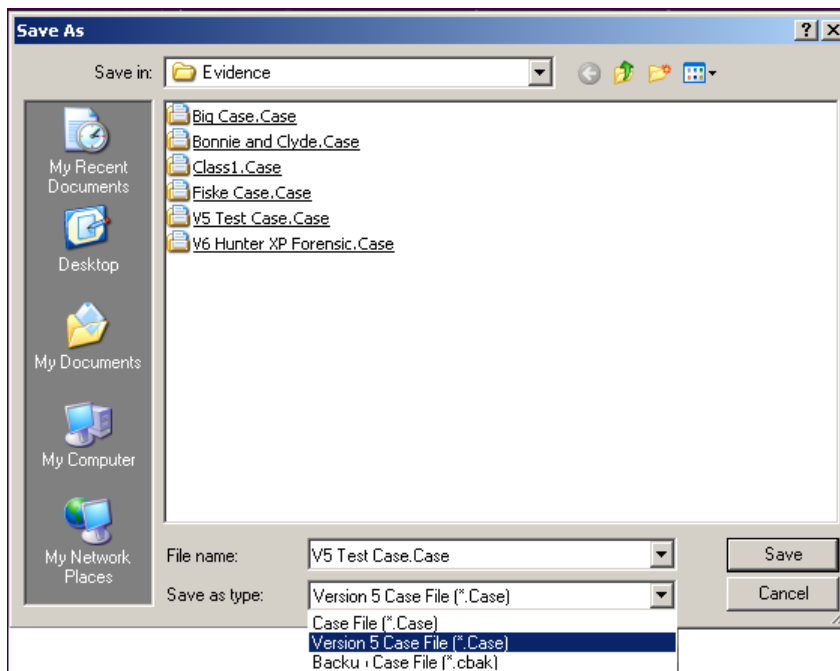
## Case File Format

Version 6 has a new case file format. As a result, case files created in version 6 do not open in previous versions. Version 6, however, does support cases created with version 5.

If a version 5 case file is opened in version 6, it can be saved as either a version 5 or a version 6 case file. You have this option in the **File > Save As** menu.

For example, a case is created in version 5, then opened and worked on in version 6. To select the version in which to save the file,

1. Select **File > Save As**.



2. Expand the **Save as type** field and make a selection.
  - ☐ **Case File** saves the file as version 6.
  - ☐ **Version 5 Case File** saves the file as version 5.
  - ☐ **Backup Case File** saves the file as a version 6 backup file.



## Case Backup

By default, a backup copy of the case file is saved every 10 minutes.

By default, backup files (.cbak) are saved to C:\Program Files\EnCase\Backup. With the exception of the extension, this file has the same name as the parent file.

To change the default save time:

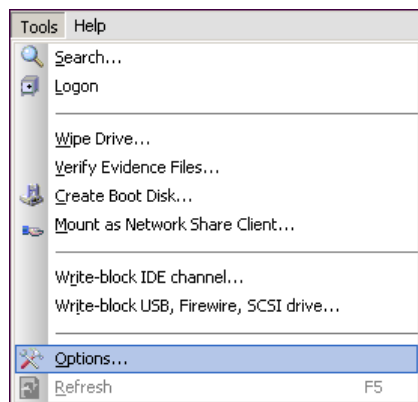
1. Select **Tools > Options > Global**.
2. Change the number in the Auto Save text field.

Selecting 0 disables the auto-save function. This is not recommended.

## The Options Dialog

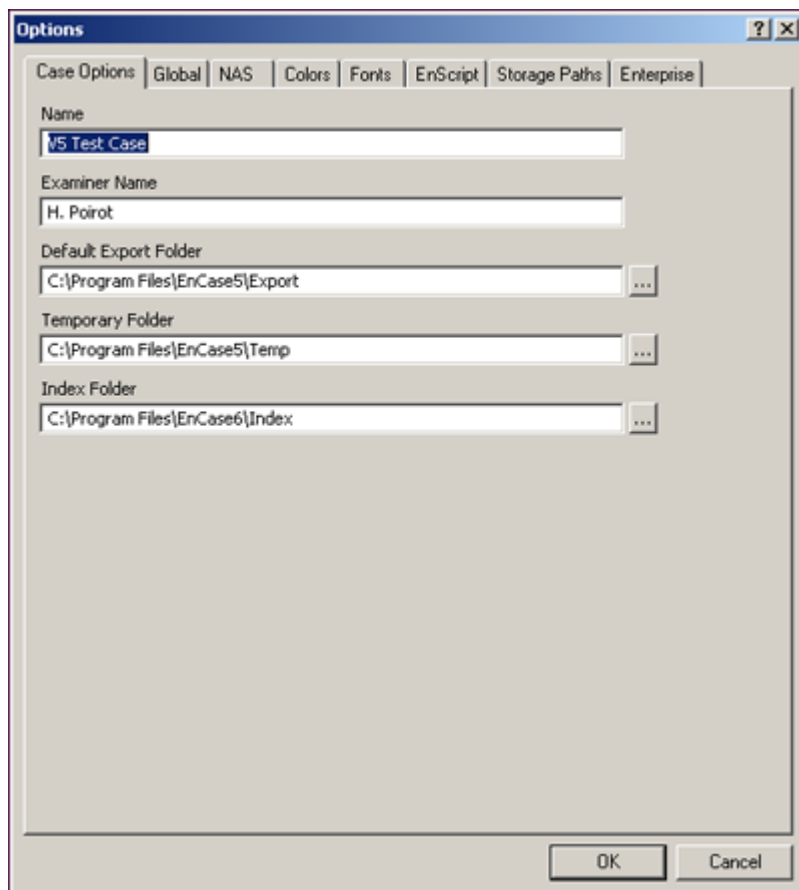
The Options menu allows you to customize the software.

To access the menu, select **Cases > Options** from the toolbar.



A tabbed dialog appears. The tabs are:

- Case Options (when a case is open)
- Global
- NAS
- Colors
- Fonts
- EnScript®
- Storage Paths
- Enterprise



---

Note: All fields on the Case Options tab are mandatory.

---

The Case Options fields in the illustration show the default values.

- **Name** holds the case name.
- **Examiner Name** is the investigator's name.
- **Default Export Folder** is the location to which exported data are sent.
- **Temporary Folder** is the location to which temporary data are sent.
- **Index Folder** is the location of case indices.

## Case Related Features

Cases use these processes:

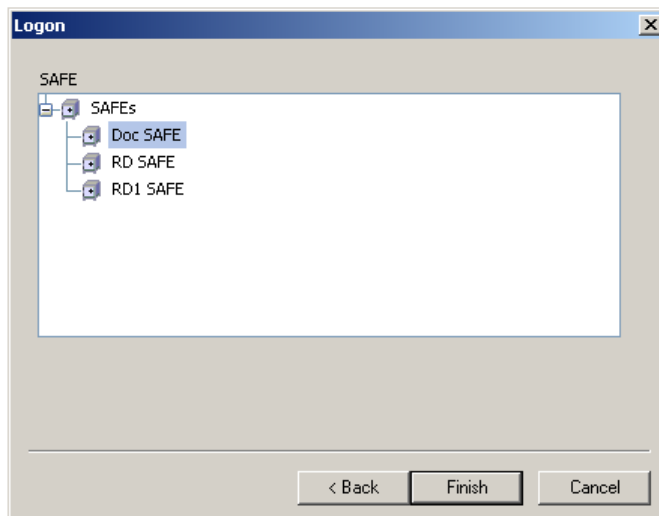
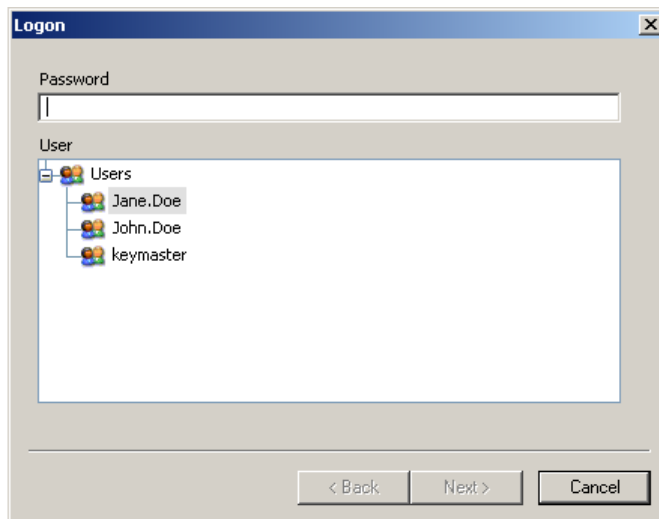
- Logon wizard
- New Case wizard
- Options dialog
- Case Time Setting dialog

## Logon Wizard

The Logon wizard captures the user name, password, and SAFE to use for the current session. The user and password are established by the administrator, or those granted administrator-level permissions.

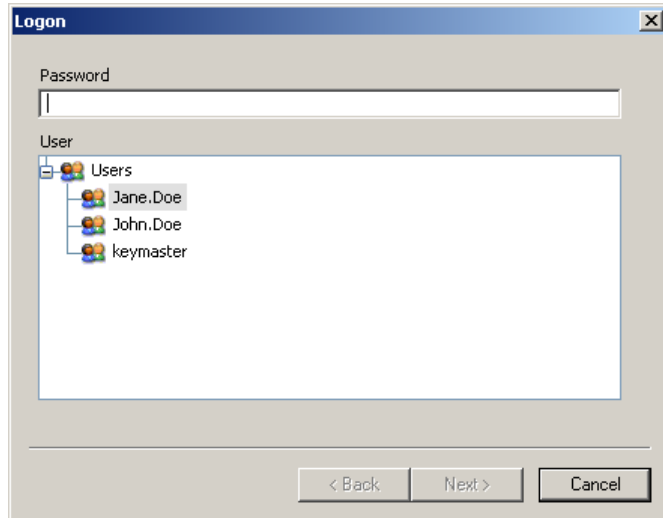
The Logon wizard displays the following pages:

- Users page
- SAFE page



## Logon Wizard Users Page

The Users page of the Login wizard captures the current user's password and user name.



**Password** captures the user password.

**User** contains the **User** tree listing users' private keys and any subfolders in the current root path. A valid user has a matching public key in the SAFE they log on to.

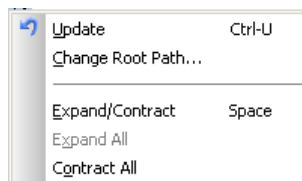
**Root User Object** provides additional functionality through a right-click menu including:

- ☐ updating the list of users displayed
- ☐ changing the root path
- ☐ commands that expand or collapse the **User** tree.

**User Objects** provides additional functionality through a right-click menu including updating the list of users displayed, and changing the root path.

## Users Right-Click Menu

The Users right-click menu provides additional functionality. The menu displays from the Users tree in the User's Page.



The **Update** command updates the Users tree display. When a user's private key is added to the default C:\Program Files\EnCase6\Keys folder or any other folder specified by the current root path, the tree does not immediately display the new user. The new user appears when the wizard is opened again, or when the User tree is updated.

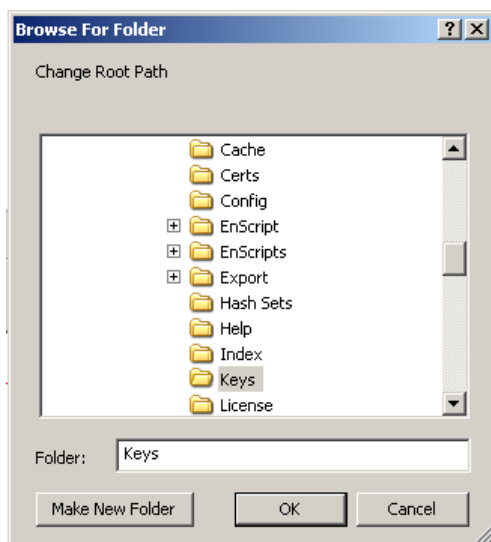
Use the **Change Root Path** command to specify a folder that contains the private keys of users other than the default folder. Specify the root path in the Browse for Folder dialog. The Users tree contains only those users in the folder specified as the new root path.

## Browse for Folder Dialog

Use this dialog to change the root path in the Users tree and the SAFE tree to specify the path to folders containing keys for users or SAFEs. The default path is C:\Program Files\EnCase6\Keys.

The Users tree is based on the private keys contained in the folder defined by the root path. The SAFE tree is based on .SAFE files contained in the folder defined by the root path. Both types of files are in the C:\Program Files\EnCase6\Keys folder.

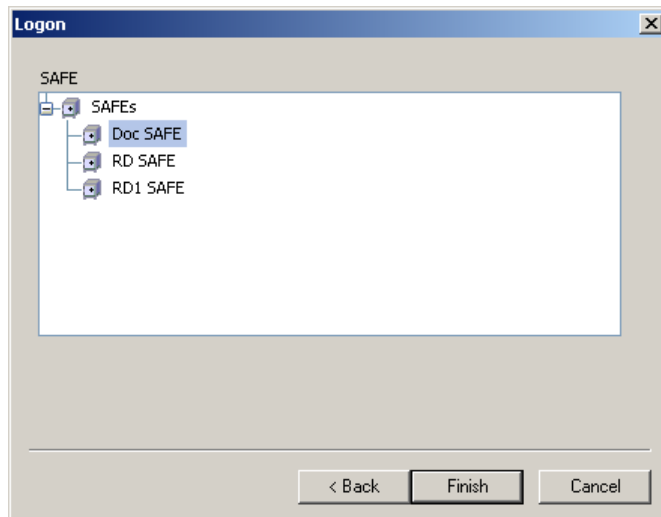
Moving these key files while the trees are displayed requires a refresh to update the trees.



Path displays a tree to navigate to the folder containing the keys.

## SAFE Page of the Logon Wizard

The SAFE page of the Logon wizard determines if SAFE is associated with and used by the current user.



**SAFE** contains the **SAFEs** tree that organizes all the SAFEs that are installed. The user selects a SAFE to complete the logon.

**SAFEs Root Object** provides additional functionality through a right-click menu such as

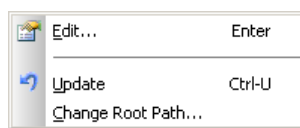
- ☐ editing the settings of the SAFE
- ☐ changing the root directory
- ☐ logging on to a remote SAFE
- ☐ additional commands that expand or collapse the **SAFEs** tree

**SAFE Objects** provides additional functionality through a right-click menu such as

- ☐ editing the settings of the SAFE
- ☐ changing the root directory
- ☐ logging on to a remote SAFE

## SAFE Right-Click Menu

The SAFE right-click menu provides additional functionality.



**Edit** opens the Edit SAFE Dialog where SAFE settings are defined and remote logons are enabled.

**Update** updates the Users tree display. When a user's private key is added to the default C:\Program Files\EnCase6\Keys folder or any other folder specified by the current root path, the tree does not immediately display the new user. The new user appears when the wizard is opened again, or when the User tree is updated.

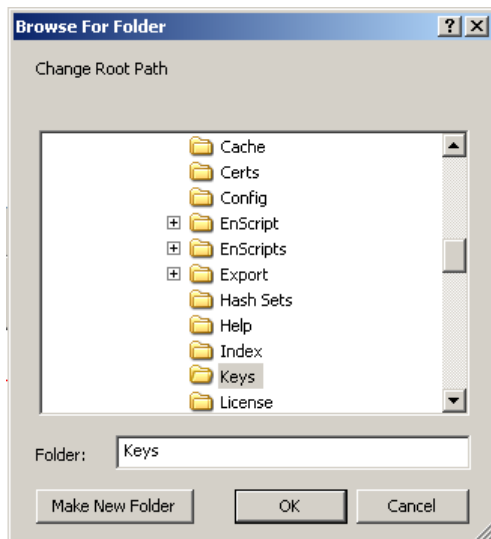
Use the **Change Root Path** command to specify a folder that contains the private keys of users other than the default folder. Specify the root path in the Browse for Folder dialog. The Users tree contains only those users in the folder specified as the new root path.

## Browse for Folder Dialog

Use this dialog to change the root path used in the Users tree and the SAFE tree to specify the path to folders containing keys for users or SAFEs. The default path is C:\Program Files\EnCase6\Keys.

The User's tree is based on the private keys contained in the folder defined by the root path. The SAFE tree is based on .SAFE files contained in the folder defined by the root path. Both types of files are found in the C:\Program Files\EnCase6\Keys folder.

Moving these key files while the trees are displayed requires a refresh to update the trees.

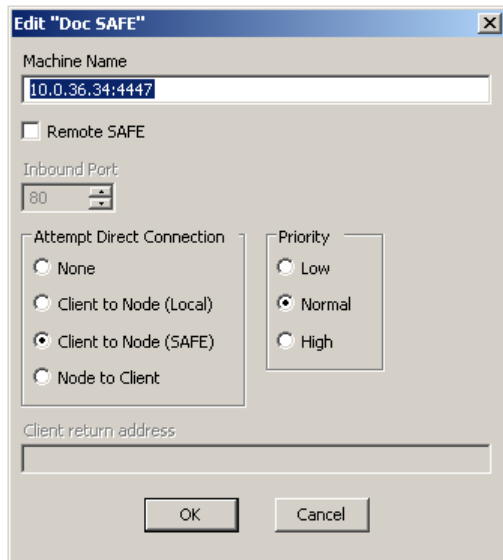


Path displays a tree to navigate to the folder containing the keys.



## Edit SAFE Dialog

The Edit SAFE dialog contains settings that define connections to the SAFE and enable remote login.



**Machine Name** contains the IP address to the machine or subnet that constitutes the SAFE or SAFEs accessed using the named SAFE.

**Remote SAFE** determines if communications with the node will be routed through the SAFE, so the SAFE stands between the client and the node. Enabling this setting allows you to provide a value for **Inbound Port** and to use its value communicating with the remote SAFE.

**Inbound Port** determines which port is used when communicating with the remote SAFE at the IP address specified in **Machine Name**.

**Attempt Direct Connection** contains settings that determine what kind of connection is made to the specified SAFE.

**None** should be enabled when the target system cannot establish a connection with an EE client. Then all traffic is redirected through the SAFE server. This can increase communication times; however, it provides the investigator with the ability to obtain data that is otherwise not available.

**Client to Node (Local)** should be enabled when the client (Examiner) and the node (servlet) reside on the same network, and the SAFE resides on a different network. This allows data to transfer directly from the node to the client, after the client successfully authenticates through the SAFE. Also the client will use the IP address that the node believes it has, rather than the IP address the SAFE has for the node. In this configuration, the network should be designed so that all the company's employees are located on the Corporate Desktop Network, and should employ routing/NATing.

**Client to Node (SAFE)** enables NAT, where a private IP address is mapped to a public IP address. Typically, the SAFE and node reside on the same subnet, and the client on another. This allows data to transfer directly from the node to the client, after the client successfully authenticates through the SAFE. The client also uses the IP address that the SAFE believes the node has, rather than the IP address the node reports it has to allow a direct connection between the client and node machine. This option is enabled by default.

**Node to Client** operates similarly to the Client to Node (SAFE) mode, except that the node attempts the direct connection to the client. It is used when you desire direct data transfer between the node and the client, and there is NATing or a firewall prohibiting the node from sending data directly to the local IP/default port of the client. Once you check this option, the Client return address configuration box becomes available to enter the NATed IP address and custom port (e.g., 192.168.4.1:1545). The Client return address box is disabled unless this option is selected.

**Priority** determines the priority of connection for this SAFE.

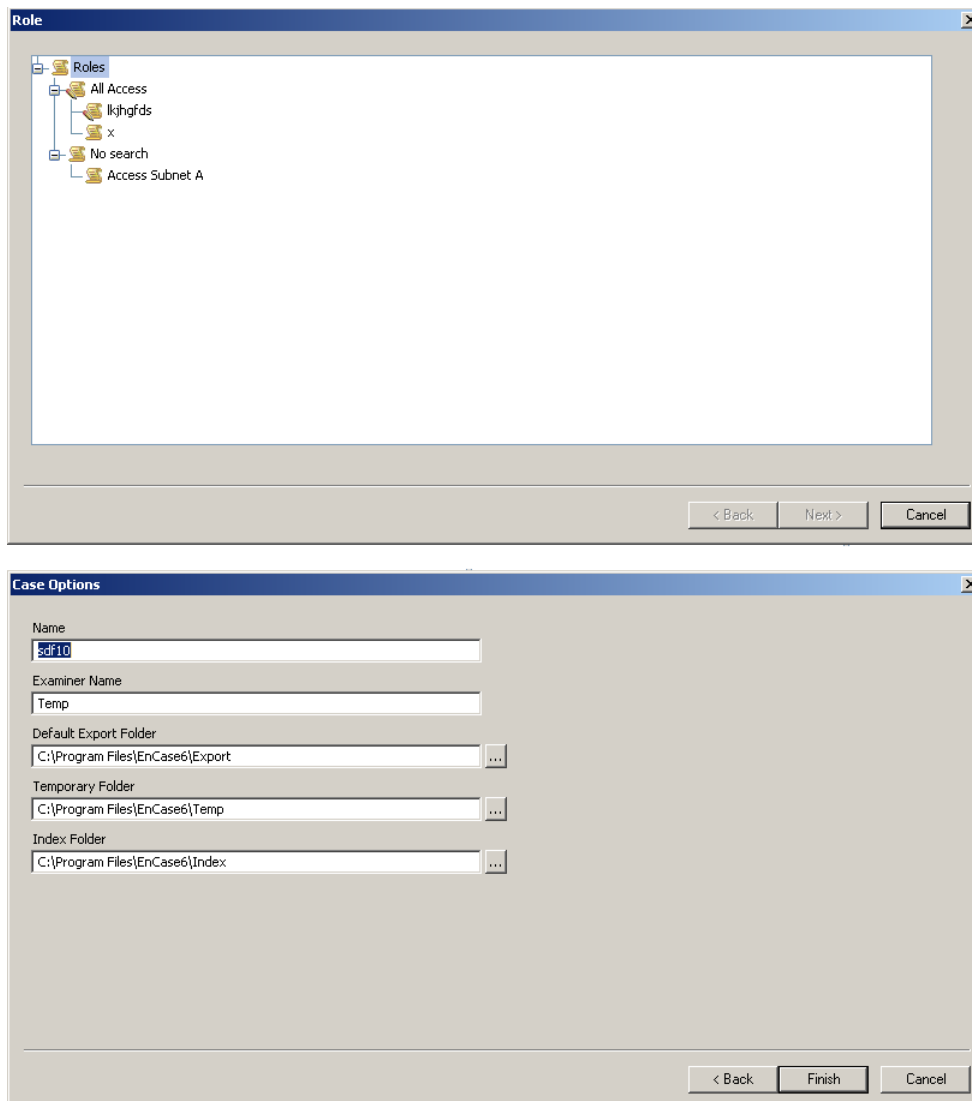
- ❑ **Low** means the connection to this SAFE will be reconnected after all other connections of normal or high priority.
- ❑ **Normal** means the connection to this SAFE will be reconnected after all other connections of high priority and before those connections of low priority.
- ❑ **High** means the connection to this SAFE will be reconnected before all other connections of medium or low priority.

## New Case Wizard

The New Case wizard captures role and case settings. A case is associated with a specific role. Roles are established by the administrator.

The New Case wizard consists of two pages:

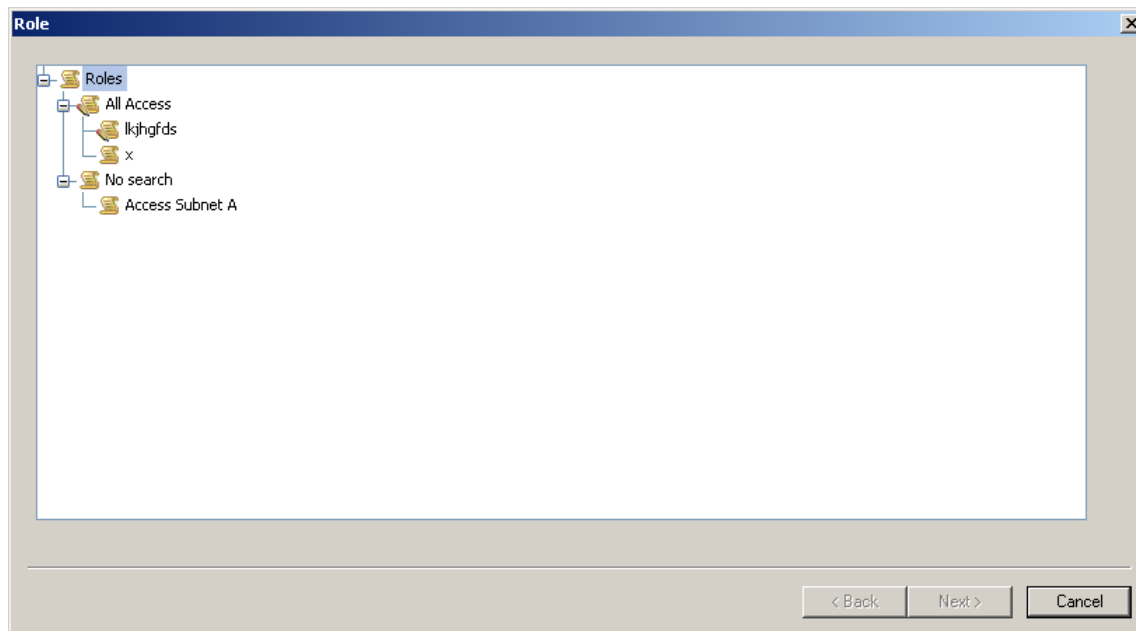
- Role page
- Case Options page



## Role Page of the New Case Wizard

The Roles page of the Login wizard associates the case being created with a role. Roles are established by the administrator.

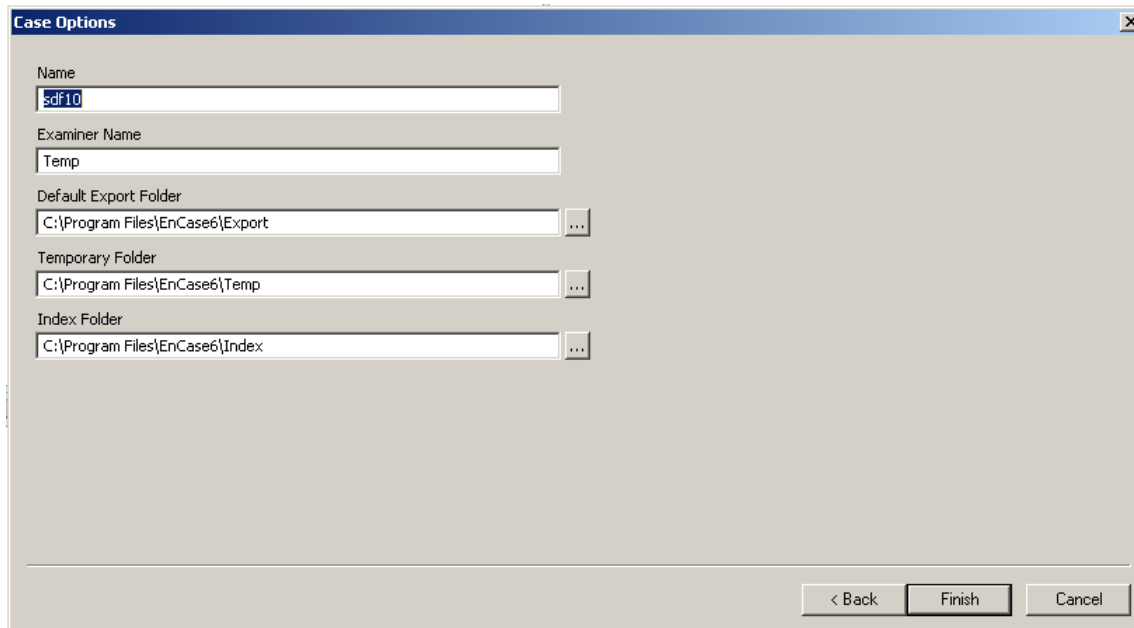
Note: Care should be taken here, because once a role is selected for a case, it cannot be changed.



**Roles** contains the Roles tree, which organizes the roles available to the user. Select the role associated with the case being created from the Roles tree.

## Case Options Page of the New Case Wizard

The Cases Options page of the New Case Wizard is where you enter the name of the case, the examiner's name and paths to folders associated with the case.



The screenshot shows the 'Case Options' dialog box. It has a title bar with the text 'Case Options' and a close button. The dialog contains five input fields, each with a label and a text box. The 'Name' field contains 'sdf10'. The 'Examiner Name' field contains 'Temp'. The 'Default Export Folder' field contains 'C:\Program Files\EnCase6\Export'. The 'Temporary Folder' field contains 'C:\Program Files\EnCase6\Temp'. The 'Index Folder' field contains 'C:\Program Files\EnCase6\Index'. Each of the three folder fields has a small button with three dots to its right. At the bottom of the dialog, there are three buttons: '< Back', 'Finish', and 'Cancel'.

**Name** contains the name of the case associated with the case options set on this tab. The case name is used as the default filename when the case is saved. You can change this filename when you save the case.

**Examiner Name** is the name of the investigator.

**Default Export Folder** contains the path to and name of the folder where files are exported.

**Temporary Folder** contains the path to and name of the folder where temporary files are created.

**Index Folder** contains the index file for any indexed file or collection of files.

## Add Device

Once a case is open, add evidence in accordance with the information in the Working with Evidence section.

## Using a Case

A case is central to an investigation. Before you can add a device, preview content, or acquire content, you must open a case. This may be a new case or an existing case.

Once you create a file, you can add a device, proceed with the device preview and acquisition, and subsequent analysis.

Use the Case Options page to define a case. The settings on this page are the same as those on the Case Options tab of the Options dialog.

Once a case is open, you can establish its time zone settings.

## Modifying Case Related Settings

Use the New Case wizard, Case Options dialog to modify case related settings after the case is created.

1. Open the case.
2. Click **Tools > Options**.  
The Case Options tab displays.
3. Change the settings through the various tabs in the Options dialog.
4. Click **OK**.

For more information, see the Installation of EnCase Enterprise chapter.

## Time Zone Settings

The Energy Policy Act of 2005 (Public Law 109-058) amends the Uniform Time Act of 1966 by changing the start and end dates of daylight saving time beginning in 2007. Clocks are set ahead one hour on the second Sunday of March, and set back one hour the first Sunday in November.

This resulting extra four weeks is called extended daylight saving time period. EnCase® software uses time zone definitions stored in the examiner's Windows registry to adjust for daylight saving time and time zone adjustments. Microsoft released a patch altering how these adjustments are stored.

The Windows registry contains a subdirectory of dynamic daylight savings time entries for different years. This allows the operating system to apply current daylight savings time settings to new files, and the corresponding year's daylight savings time for older files.

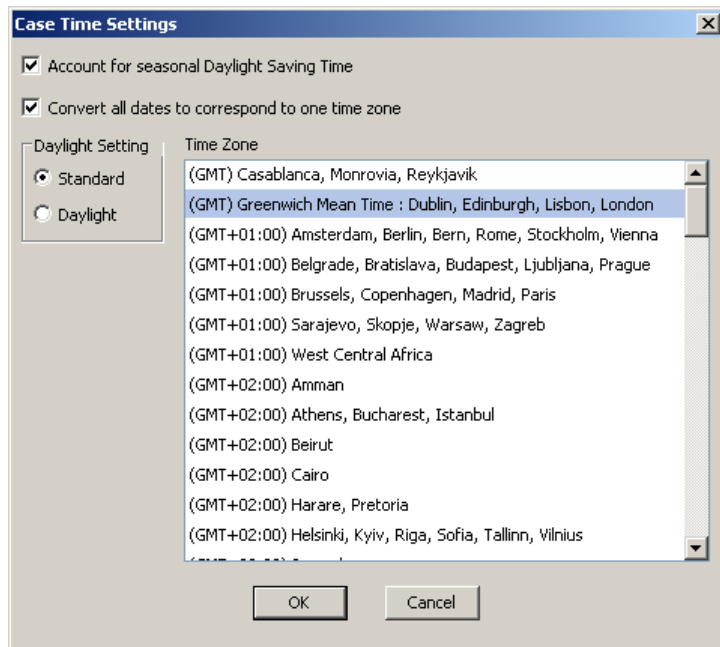
On patched machines, the root entry for daylight saving time settings is updated to the 2007 time zone settings, and that is currently the entry EnCase software uses. Therefore, if the examiner machine is patched, EnCase software uses the new 2007 rules for entries whose dates lie in the new four week extended daylight saving time period. Consequently all file dates, even those for previous years, apply the new daylight savings time settings.

Setting the time zone settings is accomplished two different ways. If you have an entire case where you want to use one time zone, you can set the time zone for the entire case. If you have several pieces of media that use different time zones, you want to set the time zones individually for each device in your case.



## Case File Time Zones

Set the time zone for the entire case with the Case Time Settings dialog.



The features of the Case Time Settings dialog are:

**Account for Seasonal Daylight Savings Time** applies DST rules as defined by the registry settings. If you want to use the new 2007 DST rules, ensure your machine is patched.

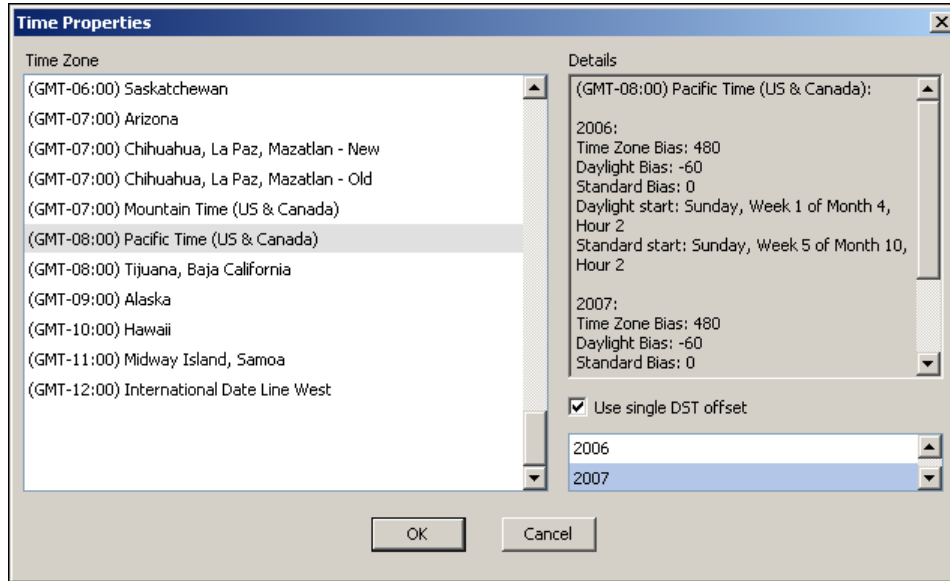
**Convert All Dates to Correspond to One Time Zone** enables the Daylight Setting and the Time Zone list. This allows you to convert all times to match one time zone.

**Daylight Setting** is disabled unless **Convert All Dates to Correspond to One Time Zone** is checked. Use the option buttons to select Standard or Daylight Savings time adjustments.

**Time Zone List** is also disabled unless **Convert All Dates to Correspond to One Time Zone** is checked. This captures the time zone you want to use with your case.

## Evidence File Time Zones

Use the Time Properties dialog to set the time zone for each evidence file.



The features of the Time Properties dialog are:

**Time Zone List** captures the time zone the subject device was set to.

**Details** provide rules used for the time zone selected in the Time Zone list. The rules listed here populate using Dynamic Daylight Savings Time, which requires that your computer is properly patched in order to use the new DST rules described above.

**Use Single DST Offset** specifies not to use Dynamic DST and instead apply a single DST offset to the entire device. Use this option when the subject machine did not have the proper 2007 DST patch described above.

**Year Selection List** is disabled until Use Single DST Offset is checked. You can select which DST rules to base the DST adjustment on:

- ☐ Use 2006 for machines using pre-2007 DST rules
- ☐ Use 2007 only on computers using the new 2007 DST rules

## Setting Time Zones Settings for Case Files

1. Open a case.
2. Click **View > Cases Sub-Tabs > Home**.

The open cases appear in the Table pane.

3. Right-click the case where for which you want to set the time zone and then select **Modify Time Settings**.

The Case Time Settings dialog displays.

4. If you want to account for seasonal daylight savings time rules, select **Account for Seasonal Daylight Saving Time**.
5. If you want to convert all dates to a particular time zone:
  - a. Select **Convert All Dates to Correspond to One Time Zone**.
  - b. Select a **Daylight Setting**.
  - c. Select a **Time Zone**.
6. When you are finished, click **OK**.

## Setting Time Zone Options for Evidence Files

1. Open a case to display its contents
2. Select a Device from the Tree pane, right-click it and choose **Modify time zone settings**.

The Time Properties dialog appears.
3. Select a Time Zone from the **Time Zone** list.

The details of the time zone appear in the **Details** text box.
4. If you want to use a single DST offset, select **Use Single DST Offset** and select the year of the DST rules you want applied.
5. When you are finished, click **OK**.

## General Time Zone Notes

- FAT, HFS, and CDFS times are not associated with any time zone when stored on a target machine. The investigator assigns a time zone to the evidence at the device level. This assignment does not change displayed dates unless a case time is set and it is different from the device time.
- NTFS and HFS+ times are associated to Greenwich Mean Time (GMT) when stored on a target machine.
- Set device time zones associates a time zone with the stored FAT times, and for NTFS displays the correct offset from GMT.
- Note: By default, all time zones are set to the examiner machine time zone.
- Modifying the case time zone to convert all times to one time zone changes the FAT, HFS, and CDFS times if the device time zone is different from that of the case time zone. All NTFS and HFS+ times are adjusted to the case GMT-offset if convert all times is applied.
- At the case level, the daylight settings respond this way:
  - ☐ If standard is selected, no change is made to any times.
  - ☐ If daylight is selected, one hour is added to all display times regardless of the time of year.
  - ☐ The investigator's system clock date in standard or daylight time should have no effect on displayed times.

## FAT, HFS and CDFS Time Zone Specifics

**FAT, HFS, CDFS:** All times are stored initially as the system time of the acquired machine. For instance, if a file is saved at 3 p.m., the time stored is 3 p.m. There is no time zone associated to 3 p.m. when the time is stored.

Setting the time zone at the device or volume level identifies the time zone in which the recorded times occurred. When the evidence is added to the program it is assumed to be in the investigator's local time.

Modifying the device level does not change times because the device time zone associates a time zone only to the times stored.

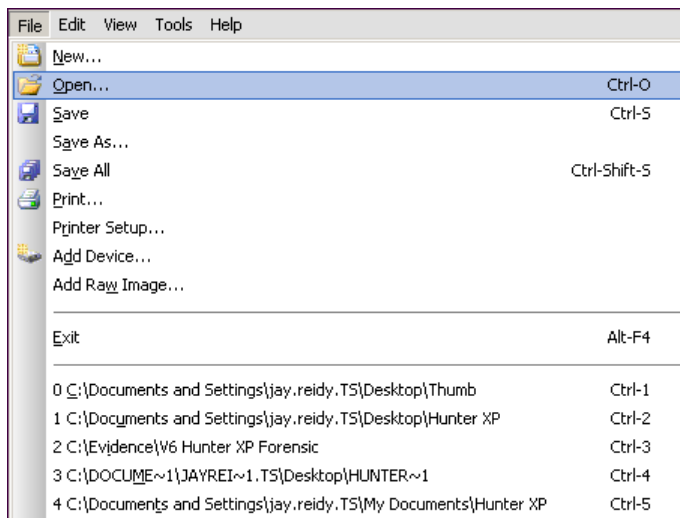
## Time Zone Example

- The target computer has an HFS in New York (-5 GMT).
- The file is created at 3 p.m. The stored time in the computer is 3 p.m.
- The drive is imaged and the investigator writes that the computer displayed the correct local time.
- An investigator in California opens the evidence file. The EnCase program initially assigns a time zone to the device level of -8 GMT since that is the time zone setting of the West coast investigator's machine. The time still displays 3 p.m. because EnCase software knows the stored time is 3 p.m. and the local time zone of the examiner is -8 GMT.

## Open a Case

Open a case to continue analysis or to review a case.

1. Select **File > Open**.



2. Browse to, or select the case from the recent files list at the bottom of the menu, and click **Open**.

---

Note: You can also open a case by double clicking the case file in Windows Explorer.

---

## Saving a Case

You can save a case:

- To its current filename and location: see *Saving a Case* (on page 176) in this document.
- With a new filename or a new location: see *Saving a Case with a New Name or New Location* (on page 176) in this document .
- To its current filename and location along with the application's current references, conditions, and filters: see *Saving a Case and the Global Application Files* (on page 176) in this document.

## Saving a Case

To save a case:

1. Click **File > Save** or click **Save** on the toolbar.

The Save dialog appears.

2. If you want to use the case name as the file name and use the default path in **My Documents**, click **Save**.
3. You can also navigate to or enter a different filename and path, and click **Save**.

## Saving a Case With a New Name or New Location

You can save any case with a new name or save it in a new location.

1. Click **File > Save As**.

The Save dialog appears.

2. If you want to use the case name or current file name and use the default path in **My Documents**, click **Save**.
3. You can also navigate to or enter a different filename and path, and click **Save**.

## Saving a Case and the Global Application Files

You can save the global application files containing preferences, conditions, and filters in the locations specified in the Storage Paths tab of the Options dialog.

1. Click **File > Save All**.  
The Save dialog appears.
2. If you want to use the current file name and the default path in `My Documents`, click **Save**.
3. You can also navigate to or enter the desired filename and path, and click **Save**.

## Close Case

Protect the integrity of cases by closing them when they are not being worked on.

1. Save the open case.
2. In Tree view, place the cursor on an open case.
3. Click **Close**.

Click **Yes** to close the case.

---

Note: Close is also available from the right-click menu.

---





# Working with Evidence

- Overview 179
- Supported File Systems and Operating Systems 182
- Using Snapshots 182
- Getting Ready to Acquire the Content of a Device 183
- Acquiring 196
- Remote Acquisition 235
- Hashing 240
- Logical Evidence Files 242
- Recovering Folders 247
- Recovering Partitions 250
- Restoring Evidence 254
- Snapshot to DB Module Set 260
- WinEn 270

## Overview

The EnCase® application organizes digital evidence into an associated case. Digital evidence is previewed, then possibly acquired. Once evidence is acquired or added to a case, it can be analyzed. In this section, we focus on previewing, acquiring, and adding digital evidence to the case.

## Types of Entries

Entries include evidence and other file types containing digital evidence that are added to a case.

There are four classes of evidence containing files that EnCase applications support:

- EnCase Evidence Files (E01)
- Logical Evidence Files (LEF/L01)
- Raw images
- Single files, including directories

These files are acquired or added to a case. Before digital evidence can be added to a case, it is previewed.

## EnCase Evidence Files

EnCase evidence files (E01) contain the contents of an acquired device and provide the basis for later analysis.

Encase evidence files integrate investigative metadata, the device-level hash value, and the content of an acquired device. This integration simplifies evidence handling and investigative efforts by keeping the device-level hash value and content together, and by simplifying the effort required to verify that the evidence has not changed since it was collected from a subject device.

Dragging and dropping an E01 file anywhere on the EnCase interface adds it to the currently opened case.

## Logical Evidence Files

Logical Evidence Files (LEF/L01) are created from files seen in a preview or existing evidence file. They are typically created after an analysis finds some noteworthy evidence.

When LEFs are verified, the stored hash value of the file is compared to the entry's current hash value.

- If the hash of the current content does not match the stored hash value, the hash is followed by an asterisk (\*).
- If no content for the entry was stored when creating the LEF, but a hash was stored, the hash is not compared to the empty file hash.
- If no hash value was stored for the entry when creating the LEF, no comparison is done, and a new hash value is not populated.

## Raw Image Files

Raw image files contain a collection of files but lack the integration of metadata and compression hash values that the EnCase evidence file provides.

Before raw image files can be acquired they must be added to a case. The Linux `dd` command is typically used to produce raw image files. Raw image files can be acquired and added to a case. During acquisition, the raw image file can be hashed and compressed. Once acquired raw image files are incorporated into an EnCase evidence file.

## Single Files

Individual files can be added to the case once **Activate Single Files** is selected.

Any file type supported by an EnCase application can be added to a case. You can do this through the interface, or through drag and drop. When files are added, they appear in the view pane.

You can add a folder containing files to a case. This can only be done using drag and drop. When you add folders, the folders appear in the entries tree and the entries table. The individual files within the folder appear only on the entries table.

## Supported File Systems and Operating Systems

What's new in this release:

- Support for the Novell File System
- UFS2 File System
- Mac DMG image files
- Updated NTFS Parser
- GUID partition tables, as implemented according to the Intel Extensible Firmware Interface (EFI) are also supported

Support for the DOS EN.EXE utility was dropped, so you should now do drive-to-drive and crossover-cable acquisitions using the LinEn utility.

## Using Snapshots

Snapshots collect a variety of information to create snapshot bookmarks. Snapshots are the output of EnScript® programs. In EnCase Forensic, only the Scan Local Machine EnScript program creates snapshots. In EnCase Enterprise, the following EnScript programs create snapshots:

- Sweep Enterprise
- Quick Snapshot

The Sweep Enterprise EnScript program captures live information from a selected network tree without a case or Enterprise logon needed before running.

The Quick Snapshot EnScript program captures live information from a selected machine associated with a device in an open case.

For more information on these EnScript programs, see *Enterprise EnScript Programs* (on page 481).

## Getting Ready to Acquire the Content of a Device

Before you can acquire the contents of a device, you must add the device, and preview the device's content.

To add, preview, or acquire the content of a device, first open the case associated with the device.

To acquire the content of a device:

1. Using the Add Device wizard, add the device.
2. Using the EnCase main window, preview the content of the device.

You are ready to acquire the contents of the device as an EnCase evidence file in the currently opened case.

### Previewing

Previewing is done before an acquisition, so an investigator can determine if the device should be acquired. A preview is not optional, although the investigator determines the extent of the preview. During a preview, the content of the device can be analyzed just as if the content had been acquired.

---

**Note:** A write blocking device, such as the FastBloc® write blocker, prevents the subject device from changing. Previewing via a crossover network cable is useful if a write blocking device is not available.

---

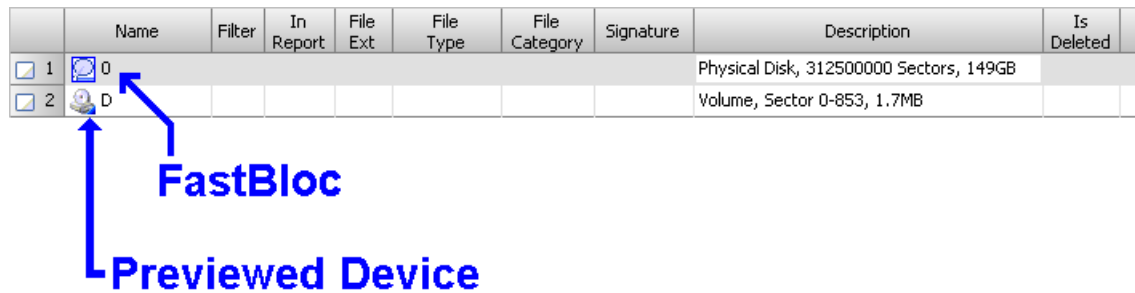
By previewing, the investigator does not have to wait to finish an acquisition before doing a preliminary examination. While previewing, you can run keyword searches, create bookmarks, perform Copy/UnErase, and other analysis functions. These search results and bookmarks can be saved into a case file, however, each time the case is opened, the subject media must be physically connected to the investigator's machine.

## Live Device and FastBloc Indicators

In the Entries Table pane and the Preview Devices page of the Add Device wizard, graphical indicators mark the devices that are previewed or blocked via Fast Block or another write blocking device.

A blue triangle in the lower right corner of the device icon indicates a previewed device.

A blue square around the device icon indicates the device is write blocked by FastBloc.



## Previewing the Content of a Device

Once devices and evidence files are added to the case file, the devices can be previewed before they are acquired.

---

Note: When a file is initially written to a multi-session CD it is assigned an offset. When the same file is changed, it is written again to the CD, as a new file in the new session, but with the same offset. Any number of revisions of the initial file are assigned the same offset. The file and all of its revisions can be viewed. Because the offset is used to associate bookmarks to the bookmarked entity, bookmarks of content on multi-session CDs will remount the first file it encounters with this offset when reopening the case.

---

Verify the device containing the content to be previewed was added to the case.

To preview the content of a device that was added to the currently opened case:

1. On the Tree pane or Table pane of the main window, look at the icon of the device being previewed to see if it is live or write blocked.
2. Perform any evidence analysis required to determine if a device should be acquired.
3. Once you have determined the device should be acquired, acquire it.

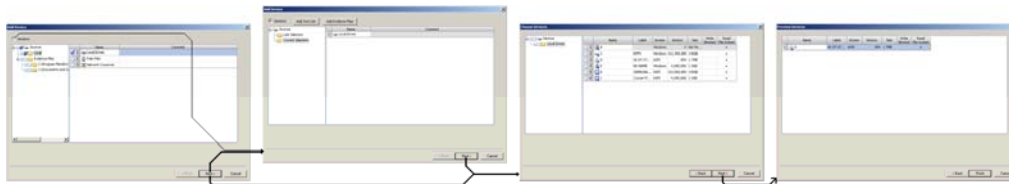
## Add Device Wizard

Use the Add Device wizard to add a device for later acquisition.

The Add Device wizard includes:

- Sources page
- Sessions Sources page (optional)
- Choose Devices page
- Preview Devices page

You must open a case before the Add Device wizard can be opened.



## Sources Page of the Add Device Wizard

You can select one or more types of sources on the Sources page of the Add Device Wizard. Local drives, a Palm Pilot, or a network crossover connection can be used as a source device for subsequent previews or acquisitions. In addition to local devices, you can add folders intended to contain evidence files.

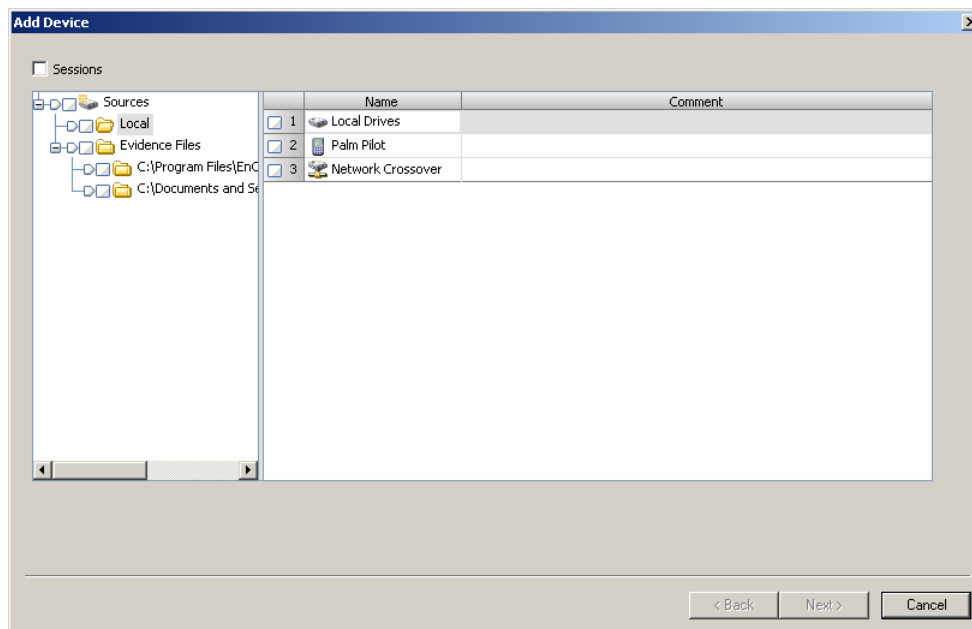
**Sessions** opens the Sessions Sources page of the Add Device Wizard when **Next** is clicked.

**Sources Tree Pane** organizes the device sources from which content is later previewed or acquired.

**Sources Root Object** contains the child objects. The right-click menu displays commands for this object. You can:

- Expand or collapse objects in the Sources tree.
- Select various objects in the Sources tree.

**Local Object** refers to local devices physically connected to the machine, which could include.





- Floppy drive
- Palm Pilot
- Removable media
- Hard drive
- Another computer

The device types appear as entries in the Table pane when the object is selected. Right-click menu commands for this object determine how to:

- Expand or collapse objects in the Sources tree
- Select various objects in the Sources tree

**Evidence Files Folder Object** contains folders added as source folders containing evidence files. The Table pane displays the same folders as the tree. The right-click menu commands for this object let you

- Add folders
- Determine which objects appear in the Sources Tree
- Determine which entries are shown in the Table pane when the object is selected

**Evidence Folder Objects** represents each folder added as a container of evidence files. As leaf nodes of the tree, the evidence files do not show in the tree, but they do appear in the Table pane. The right-click menu commands for this object let you:

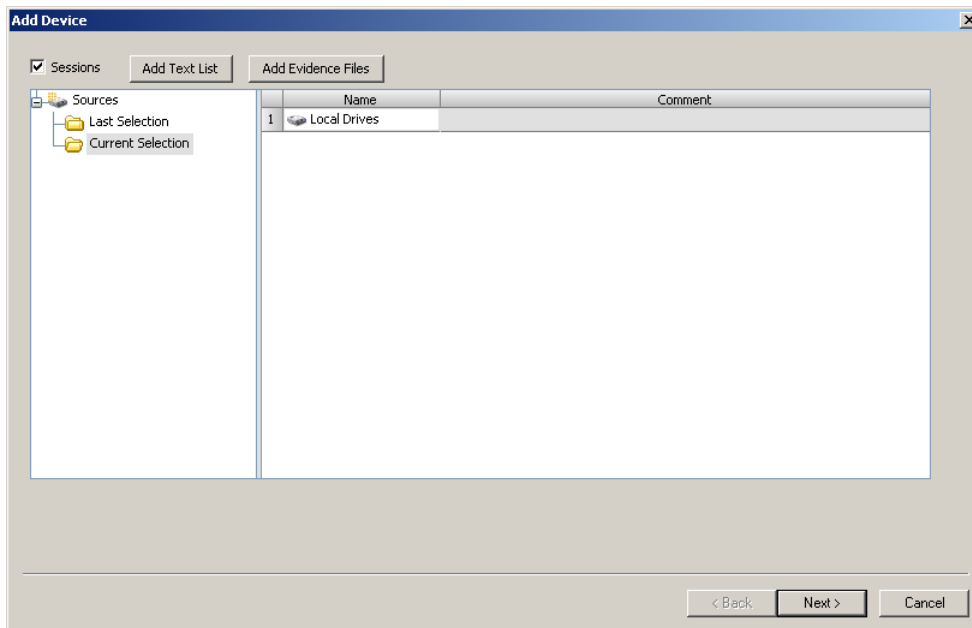
- Delete the folder where you opened the right-click menu
- Delete folders selected in the Sources tree
- Determine which objects appear in the Sources tree
- Determine which entries are shown in the Table pane when the object is selected

**Table Pane** displays the children of the currently selected folder object in the Sources tree. The right-click menu commands for this object let you

- Delete the folder where you opened the right-click menu
- Delete folders selected in the tree
- Copy the entry where you opened the right-click menu
- Select the object on the tree that corresponds to the entry where you opened the right-click menu in the Table pane
- Navigate to the parent of the object containing the entry where you opened the right-click menu in the Table pane

## Sessions Sources Page of the Add Device Wizard

When **Sessions** is enabled, you can add evidence files to the Sources tree using the Add Text List dialog or the Add Evidence Files browser.



**Sessions** opens the Sessions Sources page of the Add Device Wizard when you click **Next**.

**Add Text List** opens the Add Text List dialog, which contains a list of paths to and filenames of evidence files to be added in batch to the Sources tree.

**Add Evidence Files** opens the Add Evidence Files file browser where you can enter the path to and the filename of an evidence file, so the evidence file is added individually to the Sources tree. The following types of files can be added using this file browser:

- Evidence File (.E01)
- SafeBack File (.001)
- VMware File (.VMDK)
- Logical Evidence File (.L01)
- Virtual PC File (.VHD)

**Sources Tree** organizes the folders used to contain the evidence files added either as batch file lists or individual files. You can organize the folders in this tree hierarchically as desired.

**Sources Root Object** contains the default folders and folders added by the user that organize the evidence files either added or to be added to the Sources tree. Right-click menu commands for this object lets you:

- Add a new folder as a child
- Expand or collapse the subordinate tree

Any child objects of this object on the tree appear in as entries on the Table pane. The children of this object can be organized hierarchically by dragging and dropping folders into each other.

**Current Selection** is a default child of the Sources root object. It contains any evidence files added to the Sources tree during the current session or invocation of the Add Device Wizard. The next time the Add Device Wizard is opened, the evidence files listed here are moved to the Last Selection folder, and this folder is emptied. The right-click menu on this object lets you:

- Delete this object
- Rename this object
- Add a new folder as a child
- Expand or collapse the subordinate tree

Any child objects of this object appear as entries on the Table pane. You can organize the children of this object hierarchically by dragging and dropping folders into each other.

**Last Selection** is a default child of the Sources root object. It contains any evidence files added to the Sources tree during the prior session or invocation of the Add Device wizard. The next time the Add Device wizard is opened, the evidence files listed in the Current Selection folder are moved to this folder, and any evidence files listed before the move are removed from the folder. Once added, the evidence files continue to be used as sources until they are individually removed regardless of whether they show in the selection folders.

The right-click menu on this object lets you:

- Delete this object
- Rename this object
- Add a new folder as a child
- Expand or collapse the subordinate tree

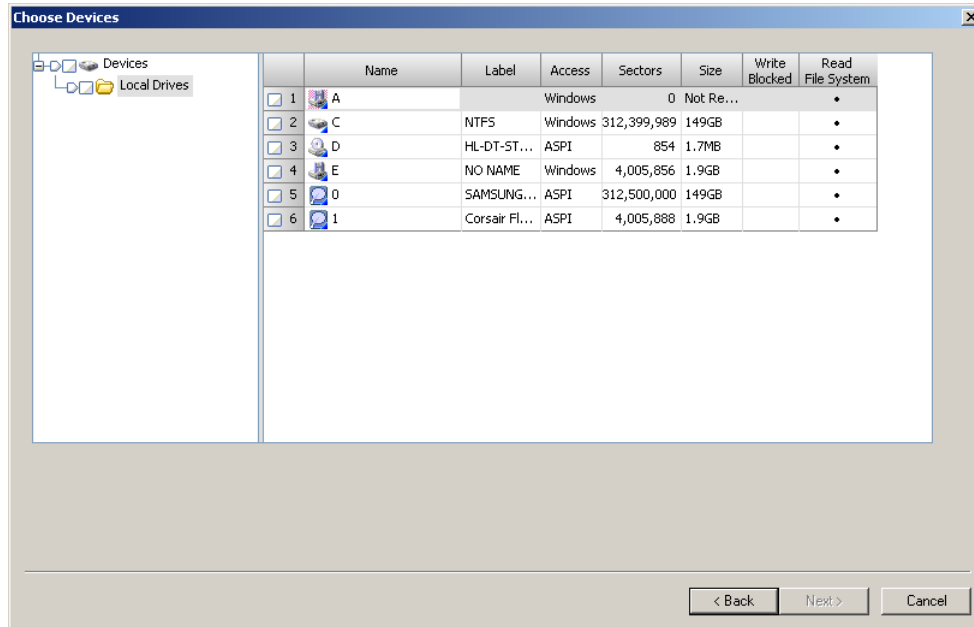
Any child objects of this object on the tree appear as entries on the Table pane. You can organize the children of this object hierarchically by dragging and dropping folders into each other.

**Table Pane** displays the children of the currently selected object in the Sources tree as entries in the table. Right-click menu commands for this object let you

- Copy an entry for use elsewhere; the copied entry cannot be pasted into the table
- Delete an entry
- Rename or edit an entry
- Navigate to the parent object of the object containing the entry

## Choose Devices Page of the Add Device Wizard

Once local devices are defined, a subset of those are selected here so they can be added to a case.



**Devices Tree** organizes the device definitions to be added to a case.

**Devices Root Object** contains the default folders that reflect the types of devices defined at this point in the *Add Device* (see "Adding a Device" on page 192) process. Right-click menu commands for this object determine:

- Which objects appear in the Sources tree
- Which entries display in the Table pane when the object is selected

**Local Drives Object** contains the current collection of child instances of the Local Drives device type entries on the Table pane. Right-click menu commands for this object determine:

- Which objects appear in the Sources tree
- Which entries display in the Table pane when the object is selected

**Table Pane** displays the children of the currently selected object in the Sources tree as entries in the table. Right-click menu commands for this object let you:

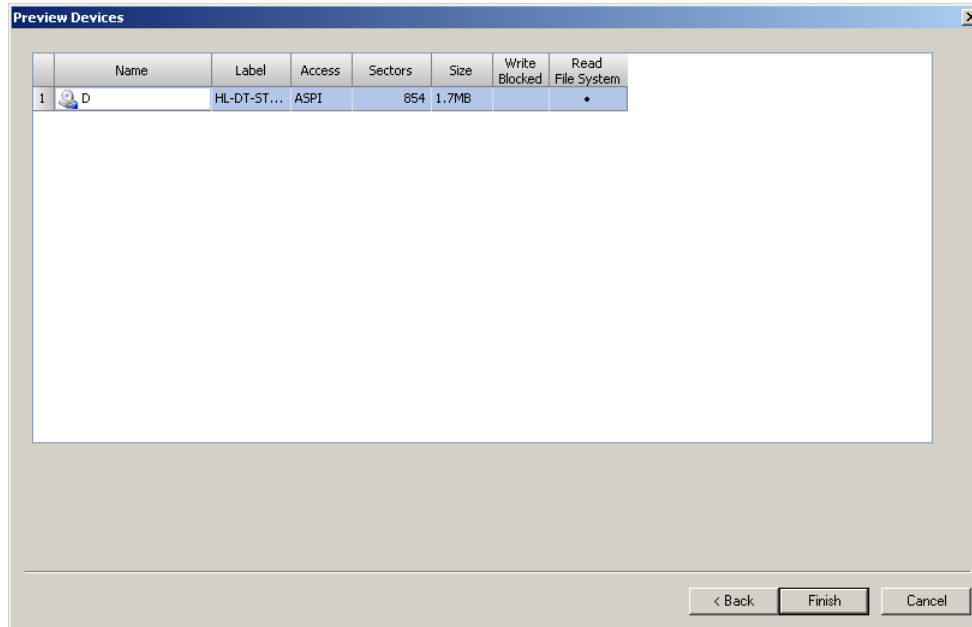
- Toggle the **Read File System Column** value
- Copy an entry for use elsewhere, as the copied entry cannot be pasted into the table
- Select an entry
- Edit an entry
- Navigate to the parent object of the object containing the entry.

**Device Selection Column** contains a check box for each row. To add a device, click its checkbox, then click **Next**.

**Read File System Column:** If this setting not selected, the file system is read in as a flat file from sector 0 to the last sector. Files, folders, and any other file system architectural structure is lost.

## Preview Devices Page of the Add Device Wizard

This page displays a list of the devices eligible to add.



**Table Pane** lists the devices that are added by clicking **Next**.

**Table Entry Rows** display the details of the device defined in that row. The right-click menu for each row provides commands that:

- Toggle the **Read File System** setting for the entry where you opened the right-click menu
- Copy the entry
- Edit the entry including the **Read File System** value. The best means to select or enable the **Read File System** is via this edit command.

**Read File System Column** when deselected, the file system is read in as a flat file from sector 0 to the last sector. Files, folders, and any other file system architectural structure is lost.

## Adding a Device

The devices added using the Add Device wizard determine the type of acquisition to be performed. The primary determiner is the device type set on the Sources Page of the Add Device wizard. The process for adding a device varies once the device type is selected.

Open a case where you want to add devices. When a case is open, the Add Device button displays on the main window tab bar.

1. Click **Add Device**.

The Sources page of the Add Device wizard appears. In the Sources tree the Local object is selected, and the local device types are listed in the Table pane.

2. Complete the Sources page of the Add Device wizard as needed, and click **Next**.

If you checked **Sessions** on the Sources page of the Add Device wizard, the Sessions Sources page of the Add Device wizard appears. Otherwise, the Choose Device page appears.

3. If **Sessions** was selected on the Sources page, complete the Sessions Sources page and click **Next**.

The Choose Device page appears.

4. Complete the Choose Device page as needed, and click **Next**.

The Preview Devices page appears.

5. Complete the Preview Devices page as needed, and click **Next**.

The devices defined and selected on the Add Device wizard are added to the currently opened case.

The devices that were added to the case can now be previewed and acquired.

## Completing the Sources Page

The Sources page of the Add Device wizard enables you to determine:

- The device types of the devices added to the case
- The evidence files added to the case

Before you begin:

- Open the case
- Open the Add Device wizard to the Sources page.

---

Note: For a local acquisition, see [Acquiring a Local Drive](#)

Note: For a Palm Pilot acquisition, see [Acquiring a Palm Drive](#)

Note: For a network crossover acquisition, see [Doing a Drive-to-Drive Acquisition in LinEn](#)

---

1. To acquire or preview a local drive:
  - a. Select the **Local** object in the Sources tree
  - b. Click the checkbox for **Local Drives** in the Table pane.
2. To acquire or preview a Palm Pilot:
  - a. Select the **Local** object in the Sources tree
  - b. Connect the Palm Pilot and set it to console mode
  - c. Click the **Palm Pilot** checkbox in the Table pane.
3. To acquire or preview a network crossover:
  - a. Select the **Local** object in the Sources tree
  - b. Start the LinEn crossover connection acquisition
  - c. If appropriate, connect the crossover connection
  - d. Click the **Network Crossover** checkbox in the Table pane.
4. To add evidence files to the case file, select **Sessions**.  
The Sessions Sources page appears after clicking **Next**.
5. Click **Next**.

If **Sessions** was selected, the Sessions Sources page appears; otherwise, the Choose Devices page appears.



## Completing the Sessions Sources Page

After the Sources page of the Add Device wizard is complete the Sessions Sources page appears.

Before you begin:

- Open the case
- Complete the Sources page in the Add Device wizard
- Select Sessions

Drag and drop an evidence file from Windows File Explorer to this page.

1. To add a list of evidence files:
  - a. Click **Add Text List**.
  - b. Enter the path and filename for each evidence file to be added using the list.
  - c. Click **OK**.
2. To add a single evidence file using a file browser:
  - a. Click **Add Evidence File**.
  - b. Browse to or enter the path and filename of the evidence file to be added.
  - c. Click **OK**.
3. If more devices need to be added, clear Sessions.

If all the devices have been added, click **Next**.

If Sessions was cleared, the Choose Devices Page appears; otherwise, the Sources page appears.

## Completing the Choose Devices Page

This page displays the devices defined that can be added to the case by the Add Device wizard.

At this point in the acquisition, the source devices were added to the Add Device wizard.

To select the subset of devices to add:

1. With an entity object selected in the Tree pane, in the Table pane select the sources to be added to the case by selecting or clearing the **Device Selection Column** checkbox for each source.
2. Click **Next**.

The Preview Devices page of the Add Device wizard appears.

## Completing the Preview Devices Page

This page displays only the selected devices from those initially defined.

Select a subset of the defined devices and evidence files so they can be added to the case.

To verify that the list of devices to be added is correct:

1. Review each row in the Table pane, and If the device attributes need to be changed, do the following:
  - a. Right-click on the row containing the device whose attributes need to be changed, and click **Edit**. The Device Attributes dialog appears.
  - b. Enter the desired changes.
2. If the device should be acquired as a flat file, clear **Read File System**.
3. Click **OK**.

The changes made in the Device Attributes dialog appear in the Table pane.

4. If the list of devices to be added is correct and complete, click **Next**; otherwise click **Back** as necessary to revise values.

The devices defined in the Add Device wizard are added to the case.

## Acquiring

Once a device is added, its contents can be acquired. Beyond an acquisition, you can add EnCase evidence files and raw evidence files to the case. Raw evidence files can be reacquired, so that they are translated into EnCase evidence files complete with metadata and hash values. Palm Pilots can also be acquired. The LinEn utility also lets you do network crossover in collaboration with EnCase Field Intelligence Model and you can use LinEn to perform disk-to-disk acquisitions. EnCase evidence files originating in other cases can be added as well.

All of these acquisitions are discussed in this section.

## Types of Acquisitions

There are several types of acquisitions that comprise EnCase evidence files (E01) and associate these files with the currently opened case.

There are several additional digital evidence file types that are associated with the currently opened case but do not involve acquisitions, except when reacquired.

There are also logical evidence files (LEF), usually constructed during a preview.

The local sources for acquisitions create E01s.

Local sources include

- Local drives (using a write blocker)
- Palm Pilot
- Network crossover (LinEn)
- Local devices (LinEn disk-to-disk)

Evidence files are added through the interface. The evidence files involved include those created by a LinEn disk-to-disk acquisition. You can add evidence files initially created for other cases to the currently opened case as well.

A network crossover acquisition involves both LinEn and the EnCase application.

LinEn disk-to-disk acquisitions create evidence files safely in the Linux environment without using a write blocker.

Dragging and dropping a file results in the file being added as a single file, rather than an evidence file. When an evidence file is dragged and dropped, it is added to the case as an evidence file.

## Doing a Typical Acquisition

A typical acquisition consists of local device acquisition using Windows and a FastBloc write blocker.

## Acquisition Wizard

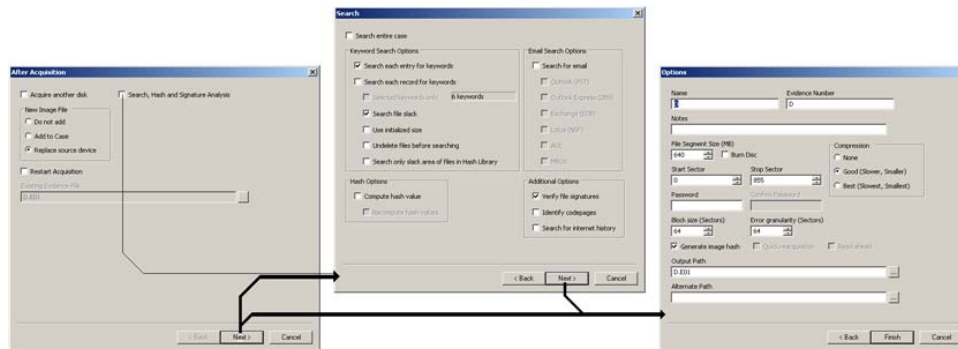
Use the Acquisition wizard to perform acquisitions.

Before acquiring a device's content, the device must be added to the case using the Add Device wizard.

The Acquisition wizard captures the specifications for the acquisition. The wizard contains the following pages:

- After Acquisition page
- (Optional) Search page
- Options page

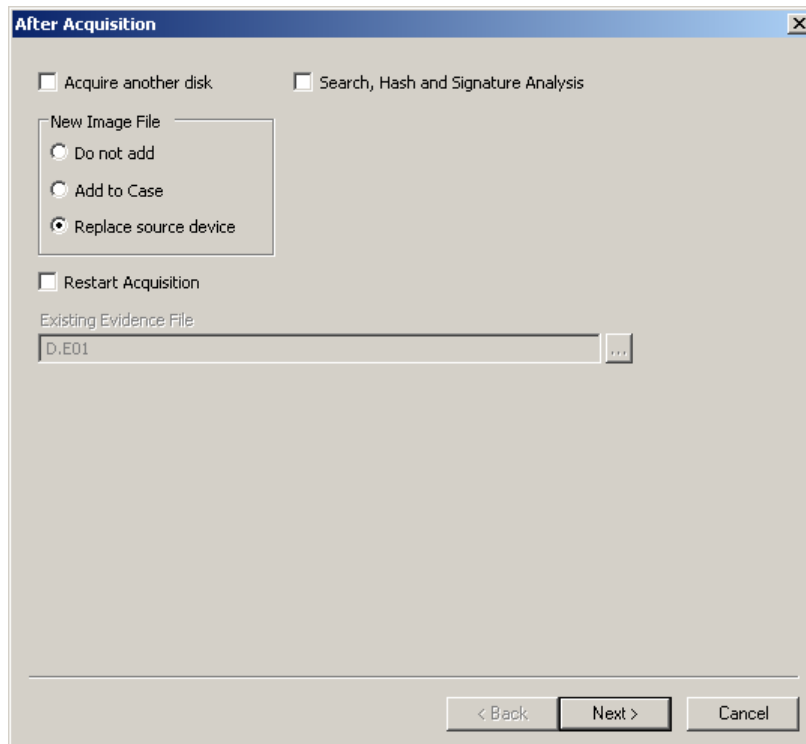
Each is explained in detail below.



## After Acquisition Page

Use the After Acquisition page of the Acquisition wizard:

- to ease the acquisition of subsequent disks
- to enable search, hash, and signature analysis to launch automatically after the acquisition is completed
- to determine what happens to the new image
- to restart a cancelled acquisition



**Acquire another disk** enables the investigator to work through a series of acquisitions (typically floppy disk content) without adding a new device for each acquisition. When **Acquire another disk** is checked:

- **Replace source device** is disabled
- **Search, Hash and Signature Analysis** is enabled.

**Search, Hash and Signature Analysis** opens the Search page of the Acquisition wizard, where search, hash and signature analysis are defined, after clicking **Next**.

**New Image File Group** controls in this group determine how the newly acquired image is saved. The default is **Replace source drive**.

**Do not add** excludes the newly acquired image from the currently opened case.

**Add to Case** adds the newly acquired image in the case file associated with the device where the image was taken.

**Replace a source device** adds the newly acquired image to the case and removes the previewed device where the acquisition was made.

**Restart Acquisition** restarts a cancelled acquisition. If the acquisition was interrupted, but not cancelled, that acquisition cannot be restarted. When you check **Restart Acquisition**, **Existing Evidence File** and its associated browse button are enabled. The file containing the data from the cancelled acquisition is available to speed up the current acquisition. The incomplete set containing the cancelled file can be replaced with a set containing all the data.

**Existing Evidence File** contains the path and filename of the evidence file whose acquisition was cancelled earlier. The existing evidence file is replaced by the acquisition in progress.

**Existing Evidence File Browse** opens the Windows file system browser to capture the path and filename of the existing evidence file.

## Search Page

Use the Search page of the Acquisition wizard to:

- Search the entire case
- Define a keyword search
- Define an email search
- Compute hash values
- Verify file signatures
- Identify codepages
- Search for internet history

Ultimately, these searches and analyses lengthen the acquisition time. For long acquisitions, these searches can be performed independently from the acquisition once the acquisition is complete.

The screenshot shows the 'Search' dialog box with the following options:

- ☒ Selected items only: 329 Entries, 0 Records
- Keyword Search Options**
  - ☐ Search entries and records for keywords
    - ☐ Selected keywords only: 10 keywords
  - ☒ Search entry slack
  - ☐ Use initialized size
  - ☐ Undelete entries before searching
  - ☐ Search only slack area of entries in Hash Library
- Hash Options**
  - ☐ Compute hash value
    - ☐ Recompute hash values
- Email Search Options**
  - ☐ Search for email
    - ☐ Recovered deleted
    - ☐ Outlook (PST)
    - ☐ Outlook Express (DBX)
    - ☐ Exchange (EDB)
    - ☐ Lotus (NSF)
    - ☐ AOL
    - ☐ MBOX
- Additional Options**
  - ☐ Verify file signatures
  - ☐ Identify codepages
  - ☒ Search for internet history
  - ☒ Comprehensive Search

Buttons: Start, Cancel

**Selected Items only** acquires only those files you checked.

**Keyword Search Options** contains controls used to define a keyword search while the content of the device is acquired.

**Search entries and records for keywords:** executes a keyword search when checked. When unchecked, other checked functions are performed, but the keyword search is not. This allows you to run a signature analysis or a hash analysis without running a keyword search. This option also enables:

- Selected keywords only
- Search entry slack
- Use initialized size
- Undelete entries before searching
- Search only slack area of entries in Hash Library

**Selected keywords only** restricts the number of keywords used during the keyword search to the number of keywords specified (shown in **Number of Keywords**).

**Search entry slack** includes file slack in the keyword search.

**Use initialized size** uses the initialized size of the device during the keyword search.

**Undelete entries before searching** undeletes deleted files before they are searched for keywords.

**Search only slack area of files in Hash Library** determines whether the slack areas of the files included in the hash library are searched.

**Hash Options** contains controls used to compute hash values.

**Compute hash value** determines whether a hash value is computed.

**Recompute hash value** determines whether a hash value is recomputed. When you recompute the hash values, they are recomputed even if hash values are already present.

**Email Search Options** contains controls used to define an email search performed while acquiring the content of the device.

**Search for email** performs an email search. This option also enables controls that determine the type of email sought.

**Recovered deleted** determines whether deleted email that remains in the PST file since the last compact operation is recovered.



**Outlook (PST)** includes .pst files in the search.

**Outlook Express (DBX)** includes .dbx files in the search.

**Exchange (EDB)** includes .edb files in the search.

**Lotus (NSF)** includes .nsf files in the search.

**AOL** includes AOL email files in the search.

**MBOX** includes MBOX email files in the search.

**Additional Options** contains controls that determine additional analysis to perform on the content being acquired.

**Verify file signatures** authenticates file signatures during the acquisition.

**Identify codepage:** If you check this option, the software attempts to determine the codepage of each file, then saves those codepages for later use in the view pane when the file contents are displayed.

**Search for internet history** finds Internet history files during the acquisition.

## Options Page

The Options page of the Acquisition wizard defines the metadata and various aspects of the image generated by the acquisition, which constitutes the EnCase evidence.

The screenshot shows the 'Options' dialog box in the EnCase Acquisition wizard. The dialog has a title bar with 'Options' and a close button. It contains several input fields and checkboxes for configuring the acquisition process. The 'Name' field is set to 'D' and the 'Evidence Number' field is also set to 'D'. The 'Notes' field is empty. The 'File Segment Size (MB)' is set to 640, and the 'Burn Disc' checkbox is unchecked. The 'Start Sector' is 0 and the 'Stop Sector' is 855. The 'Password' and 'Confirm Password' fields are empty. The 'Block size (Sectors)' is 64 and the 'Error granularity (Sectors)' is 64. The 'Compression' section has three radio buttons: 'None', 'Good (Slower, Smaller)' (which is selected), and 'Best (Slowest, Smallest)'. The 'Generate image hash' checkbox is checked, while 'Quick reacquisition' and 'Read ahead' are unchecked. The 'Output Path' is 'D:E01' and the 'Alternate Path' is empty. At the bottom, there are three buttons: '< Back', 'Finish', and 'Cancel'.

Field/Option	Value/Setting
Name	D
Evidence Number	D
Notes	
File Segment Size (MB)	640
Burn Disc	<input type="checkbox"/>
Start Sector	0
Stop Sector	855
Password	
Confirm Password	
Block size (Sectors)	64
Error granularity (Sectors)	64
Generate image hash	<input checked="" type="checkbox"/>
Quick reacquisition	<input type="checkbox"/>
Read ahead	<input type="checkbox"/>
Output Path	D:E01
Alternate Path	
Compression	Good (Slower, Smaller)

**Name** contains the name of the EnCase Evidence File that contains the image resulting from the acquisition of the underlying device.

**Evidence Number** contains the investigator-assigned number for the EnCase evidence file produced by the acquisition in progress.

**Notes** contains the investigator's notes regarding this EnCase evidence file.

**File Segment Size** specifies file segment size of the evidence files. It is useful for controlling the size of evidence files.

**Start Sector** specifies the first sector of the content you want to acquire.

**Stop Sector** specifies the last sector of the content you want to acquire.

**Password** determines if the EnCase evidence file is password protected, and what password is used. Entering a password enables **Confirm Password**. This password cannot be reset.

**Block size** determines the block size of the contents where CRC values are computed.

**Error granularity** determines the portion of the block is zeroed out if an error is encountered. The error granularity will be at the most the same value as **Block size**, or an even fraction of **Block size**.

**Quick reacquisition** allows you to quickly reacquire in order to change the file segment size, or to apply or remove a password.

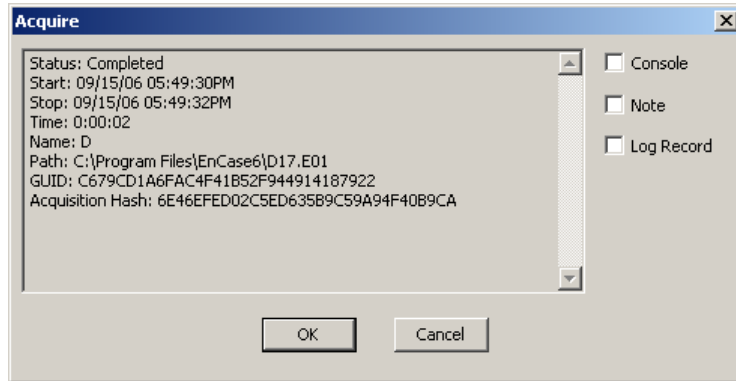
**Read Ahead** reads the acquired content, so that errors can be detected before the block is acquired, or CRCs are calculated and hashed.

**Output Path** determines the path and filename where the EnCase evidence file resulting from the acquisition is written.

**Alternate Path** contains the path and filename of an alternative destination volume where the EnCase evidence file is stored if the first location runs out of disk space.

## Acquisition Results Dialog

This dialog displays while an acquisition is performed.



**Console** sends the status messages displayed in the dialog to the Console tab of the view.

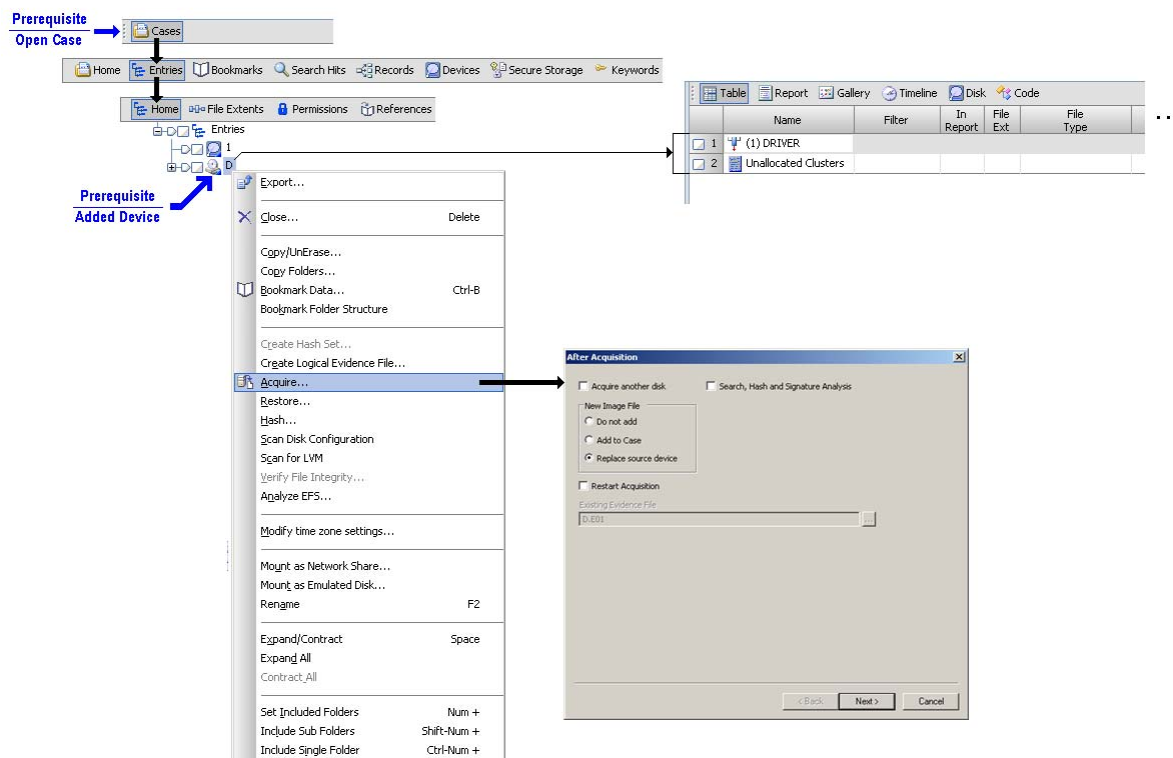
**Note** writes the contents of the status message into a bookmark note containing the device and EnCase evidence file being acquired.

**Log Record** adds the status messages displayed to a bookmark log record.

## Opening the Acquisition Wizard

Before you begin:

Open the case associated with the EnCase evidence file before you acquire an EnCase evidence file. The device from which the content is acquired must already be added to the case.



*To open the Acquisition wizard:*

1. To reach the Entries tree, in the Tree pane, click **Cases > Entries > Home**.

The Entries tree displays in the Tree pane.

2. In the Entries tree, highlight the desired device.
3. Right-click the highlighted device object.

The Device right-click menu appears.

4. Click **Acquire**.

The Acquisition wizard appears.

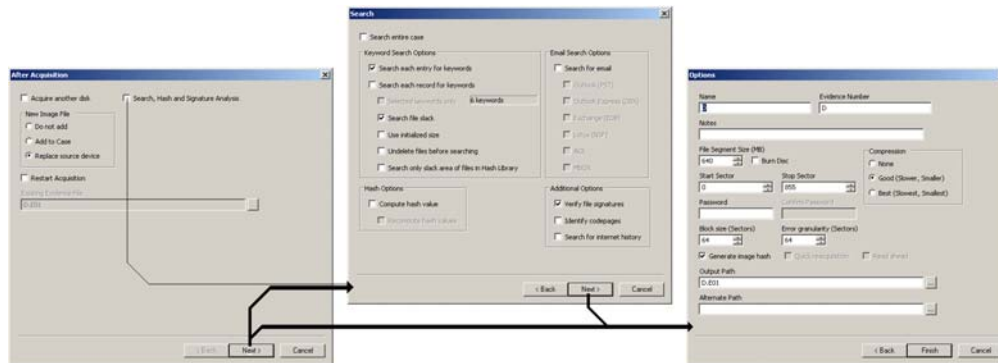
Continue creating an EnCase evidence file by completing the acquisition specification using the Acquisition wizard.

## Specifying and Running an Acquisition

This completes creation of an EnCase Evidence File.

Before you begin:

Open the After Acquisition page of the Acquisition wizard.



To specify and run the acquisition:

1. As needed, change the default settings on the After Acquisition page as described in Completing the After Acquisition Page of the Acquisition Wizard.
2. Click **Next**.

If you selected **Search, Hash and Signature Analysis**, the Search page of the Acquisition wizard appears. Otherwise, the Options page of the Acquisition wizard appears.

3. If the Search page appeared: as needed,
  - ☐ Change the default settings on the Search page, described in Completing the Search Page of the Acquisition Wizard
  - ☐ Click **Next**.

The Options page of the Acquisition wizard appears.

4. As needed:
  - ☐ Change the default settings on the Options page, described in Completing the Options Page of the Acquisition Wizard
  - ☐ Click **Finished**.

The acquisition begins.

If the file is to be saved in the case, the CRCs are verified, and any after-acquisition processing is performed.

The thread statuses for the acquisition, verification, and post processing is displayed as the processes execute.

Once the processes are complete, the results dialog appears. While the acquisition is running, the acquisition can be cancelled (see [Cancelling an Acquisition](#)).

---

Note: The evidence file containing both the content of the device and its associated metadata is saved as determined by the New Evidence File on the After Acquisition page of the Acquisition Wizard.

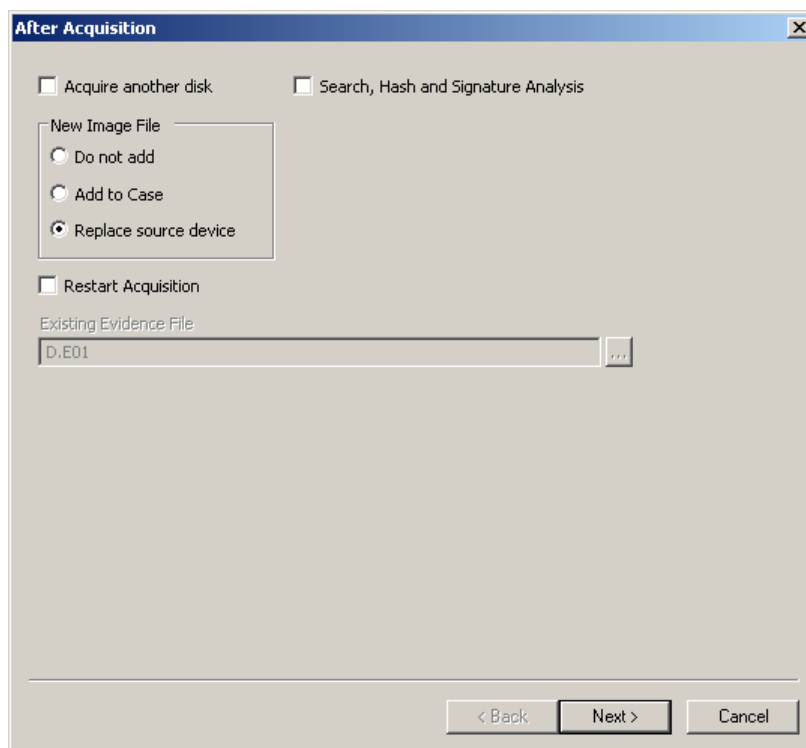
---

## Completing the After Acquisition Page of the Acquisition Wizard

This page of the Acquisition wizard specifies the actions taken once the content has been acquired, but before the acquisition is completed.

Before you begin:

Open the Acquisition wizard to the After Acquisition page.



*To define actions after the acquisition:*

1. If additional disks are to be acquired after this acquisition, select **Acquire another disk**.  
When **Acquire another disk** is acquired, the image associated with that disk is added to the case, and the **New Image File** value is set to reflect this.
2. If the content being acquired is to be searched, hashed, or analyzed for signatures, select **Search, Hash and Signature Analysis**.

3. Click **Next**. The Search page of the Acquisition Wizard appears.
4. In **New Image File**, click on the appropriate disposition of the file containing the acquired image.
5. If you want to restart a cancelled acquisition:
  - a. Select **Restart Acquisition**.
  - b. Browse to or enter the filename and path of the EnCase evidence file containing the partial acquisition to be restarted.
6. Click **Next**.

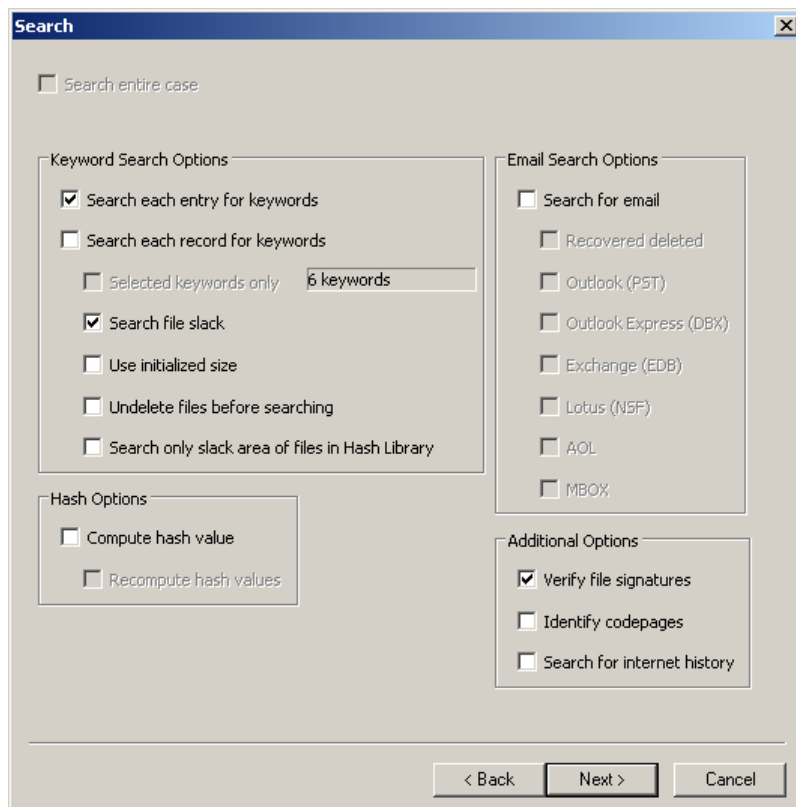
If you selected **Search, Hash and Signature Analysis**, the Search page of the Acquisition wizard appears; otherwise, the Options page appears.

## Completing the Search Page of the Acquisition Wizard

This page defines the searches, hashing, and additional analysis performed as part of the acquisition after the content is acquired.

Before you begin:

Open the Acquisition Wizard to the Search page.





To define the analysis processing as part of the acquisition:

1. Do the following as required:
  - ☐ To search all the content of devices associated with the case, not just the content of the device being acquired, click **Search entire case**.
  - ☐ To perform a keyword search, click the appropriate controls in the **Keyword Search Options**.
  - ☐ To perform an email search, click the appropriate controls in **Email Search Options**.
  - ☐ To compute or recompute hash values, click the appropriate controls in **Hash Options**.
  - ☐ To verify file signatures, in **Additional Options**, click **Verify File signatures**.
  - ☐ To identify codepages, in **Additional Options**, click **Identify codepages**.
  - ☐ To search for internet history files, in **Additional Options**, click **Search for internet history**.
2. Click **Next**.

The Options page of the Acquisition wizard appears.

## Completing the Options Page of the Acquisition Wizard

This page of the Acquisition Wizard specifies how the EnCase evidence file is built during the acquisition, and the disposition of that file after the Acquisition is complete.

The 'Options' dialog box is shown with the following fields and controls:

- Name:** A text field containing 'D'.
- Evidence Number:** A text field containing 'D'.
- Notes:** A large text area.
- File Segment Size (MB):** A spinner box set to 640.
- Burn Disc:** An unchecked checkbox.
- Start Sector:** A spinner box set to 0.
- Stop Sector:** A spinner box set to 855.
- Password:** A text field.
- Confirm Password:** A text field.
- Compression:** A group box containing three radio buttons: 'None' (unchecked), 'Good (Slower, Smaller)' (selected), and 'Best (Slowest, Smallest)' (unchecked).
- Block size (Sectors):** A spinner box set to 64.
- Error granularity (Sectors):** A spinner box set to 64.
- Generate image hash:** A checked checkbox.
- Quick reacquisition:** An unchecked checkbox.
- Read ahead:** An unchecked checkbox.
- Output Path:** A text field containing 'D:E01' with a browse button (...).
- Alternate Path:** A text field with a browse button (...).
- Buttons:** '< Back', 'Finish', and 'Cancel' at the bottom.

To define how the EnCase evidence file is built and output:

1. Accept the default values or enter or select alternative values.
2. Enter an **Evidence Number** and **Notes**.
3. If a hash has not been requested yet and one is desired, click **Generate image Hash**.
4. If you might run out of storage space where you are storing the acquired device, specify additional storage by browsing to or entering a path and filename in **Alternate Path**.
5. Click **Finish**.

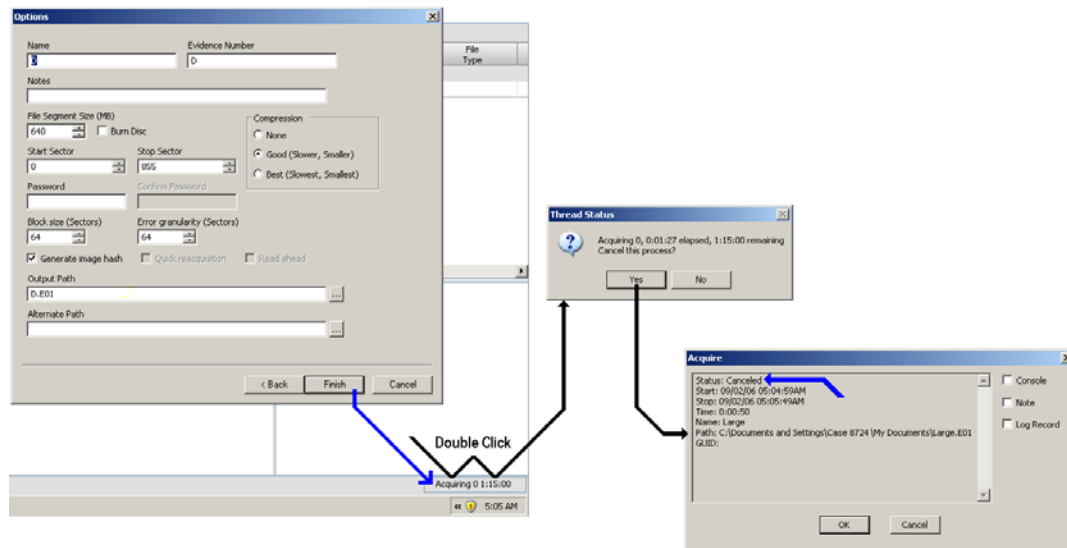
The acquisition starts, and the **Thread Status Line** appears at the bottom right corner of the main window displaying the status of the thread performing the acquisition. You can cancel the acquisition during processing (see Cancelling an Acquisition).

6. When the Acquisition Results dialog displays a status of finished, select **Console**, **Note**, or **Log Record**.
7. Click **OK**.

The Acquisition Results dialog closes and the acquisition is complete.

## Canceling an Acquisition

You can cancel an acquisition while an Acquisition is running. After canceling, the Acquisition can be restarted. If, however, the acquisition ends without being cancelled, you cannot restart it.



### *To cancel an acquisition while it is running*

1. At the bottom right corner of the main window, double-click the Thread Status Line. The **Thread Status message** box appears.

2. Click **Yes**.

The Acquisition Results dialog appears displaying cancelled status.

3. Click **Ok**.

The acquisition is cancelled. You can restart it at a later time.

## Acquiring a Local Drive

Before you begin:

The local drive to be acquired was added to the case.

1. To protect the local machine from changing while its content is being acquired, use a write blocker (see Using a Write Blocker), then verify that the device being acquired is shown in the Tree pane or the Table pane as write protected, (see Live Device and FastBloc Indicators).
2. Perform the acquisition (see Specifying and Running an Acquisition).

The drive is acquired.

## Acquiring Device Configuration Overlays (DCO) and Host Protected Areas (HPA)

EnCase applications can detect and image DCO and/or HPA areas on any ATA-6 or higher-level disk drive. These areas are detected using LinEn (Linux) or the FastBloc SE module. EnCase applications running in Windows with a hardware write blocker will not detect DCOs or HPAs.

EnCase applications using

- FastBloc SE
- LinEn when the Linux distribution used supports Direct ATA mode

The application now shows if a DCO area exists in addition to the HPA area on a target drive. FastBloc SE is a separately purchased component.

HPA is a special area located at the end of a disk. It is usually configured so the casual observer cannot see it, and it can only be accessed by reconfiguring the disk. HPA and DCO are extremely similar: the difference is the SET\_MAX\_ADDRESS bit setting that allows recovery of a removed HPA at reboot. When supported, EnCase applications see both areas if they coexist on a hard drive. For more information, see the EnCase Modules Manual.

## Using a Write Blocker

Write blockers prevent inadvertently or intentionally writing to an evidence disk. Their use is described in these sections:

- Windows-based Acquisitions with FastBloc Write Blockers
- Acquiring in Windows Without FastBloc
- Windows-based Acquisitions with a non-FastBloc Write Blocker

FastBloc supports AMD 64-bit architecture. By replacing the existing IDE and SCSI controller driver with the new Guidance driver, only read-only requests are sent to the attached hard drives.

The FastBloc® SE Module can be used with devices equipped with the Promise® SATA cards

- 300 TX4302
- 300 TX4
- 300 TX2PLUS

There is also support for the AMD Athlon™ 64 processor, and for systems running Microsoft Windows XP 64-bit edition, and Microsoft Windows Server 2003 64-bit edition.

## Windows-based Acquisitions with FastBloc Write Blockers

The following write blockers are supported in EnCase Enterprise v6.0:

*Figure 25 FastBloc FE*



*Figure 26 FastBloc 2 FE v1*



*Figure 27 FastBloc 2 FE v2*



*Figure 28 FastBloc LE*



Figure 29 FastBloc 2 LE



Computer investigations require a fast, reliable means to acquire digital evidence. FastBloc Lab Edition (LE) and FastBloc Field Edition (FE) (hereafter referred to as FastBloc) are hardware write-blocking devices that enable the safe acquisition of subject media in Windows to an EnCase evidence file. Before FastBloc was developed, noninvasive acquisitions were exclusively conducted in cumbersome command-line environments.

The hardware versions of FastBloc are not standalone products. When attached to a computer and a subject hard drive, FastBloc provides investigators with the ability to quickly and safely preview or acquire data in a Windows environment. The unit is lightweight, self-contained, and portable for easy field acquisitions, with on-site verification immediately following the acquisition.

FastBloc SE is a software version of this product.

## Acquiring in Windows Without a FastBloc Write Blocker

Never acquire hard drives in Windows without FastBloc because Windows writes to any local hard drive visible to it. Windows will, for example, put a Recycle Bin file on every hard drive that it detects and will also change Last Accessed date and time stamps for those drives.

Media that Windows cannot write to is safe to acquire from within Windows, such as CD-ROMs, write-protected floppy diskettes, and write-protected USB thumb drives.

## Windows-based Acquisitions with a non-FastBloc Write Blocker

EnCase applications cannot recognize the presence of any hard drive writeblocker other than FastBloc. For that reason, EnCase will report that the subject hard drive is not protected, when it might be. Users of non-FastBloc writeblockers are encouraged to test their equipment and become familiar with their capabilities.

## Performing a Drive-to-Drive Acquisition Using LinEn

Once LinEn is set up, run LinEn, choose **Acquire**, then select the drive to be acquired and the storage path. Optionally, provide additional metadata.

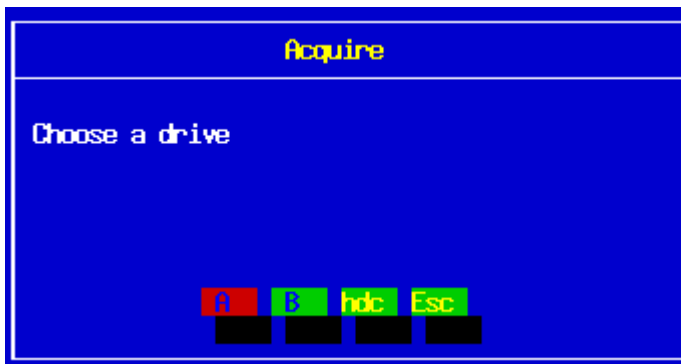
LinEn was configured as described in LinEn Setup, and **autofs** is disabled (cleared).

The investigator identifies the subject drive to be acquired and the storage drive that will hold the acquired evidence file.

1. If the FAT32 storage partition to be acquired has not been mounted, mount it.
2. Navigate to the folder where LinEn resides and type `./linen` in the console to run LinEn. The LinEn Main Screen appears.

EnCase (6.0) (Linux)								
Code	Type	Sectors	Size	LP	Label	System	Size	
Disk0 /dev/hda Linux 78165360 Sectors Size 37.3GB				hda1	/dev/hda1	Linux	498.1MB	
00	82	Linux Swap	1020096	498.1MB	hda2	/dev/hda2	Linux	10.0GB
00	83	Linux EXT2	20972448	10.0GB	hda3	/dev/hda3	Linux	4.7GB
00	83	Linux EXT2	9766512	4.7GB	hda4	/dev/hda4	Linux	22.1GB
00	0C	FAT32X	46406304	22.1GB	hdd1	/dev/hdd1	Linux	19.5GB
Disk5 /dev/hdd Linux 234375120 Sectors Size 111.8GB				hdd2	/dev/hdd2	Linux	29.3GB	
00	0C	FAT32X	40965750	19.5GB	hdd3	/dev/hdd3	Linux	31.2GB
00	0C	FAT32X	61432560	29.3GB	sda1	/dev/sda1	Linux	31.4MB
00	0C	FAT32X	65529135	31.2GB				
Disk9 /dev/sda Linux 64000 Sectors Size 31.2MB								
80	04	FAT16	64448	31.5MB				
<div>acquire</div> <div>ash Ser er uit</div>								

3. Choose **Acquire**. The Acquire screen appears.



4. Choose the physical drive or logical partition you wish to acquire. The Acquire Device <drive> dialog appears.





5. For the data elements requested by the Acquire dialog, either accept the default when provided, or enter a value or choose one of the alternatives (see Specifying and Running an Acquisition section), and then press **Enter**.

The Acquire Device dialog requests additional data values until all data elements are entered or selected. Then the Creating File dialog appears.

6. When the acquisition is complete, click **OK**.

The LinEn main window appears. The subject was acquired and is stored on the storage drive.

7. Connect the storage drive to investigator's machine.
8. Add the EnCase evidence file using the Sessions Sources page of the Add Device Wizard (see Completing the Sessions Sources Page).

## Acquiring a Disk Running in Direct ATA Mode

If the Linux distribution supports the ATA mode, you will see a **Mode** option. The mode must be set before the disk is acquired. An ATA disk can be acquired via the drive-to-drive method. The ATA mode is useful for cases when the evidence drive has a Host Protected Area (HPA) or drive control overlay (DCO). Only Direct ATA Mode can review and acquire these areas.

LinEn is been configured as described in Linen Setup, and **autofs** is disabled (cleared). Linux is running in Direct ATA Mode.

1. If the FAT32 storage partition to be acquired has not been mounted, mount it.
2. Navigate to the folder where LinEn resides and type `./linen` in the console.

The LinEn Main Screen appears.

3. Select **Mode**, then select Direct ATA Mode.

You can now acquire the disk running in ATA mode.

4. Continue the drive-to-drive acquisition with Step 3 of Doing a Drive-toDrive Acquisition Using LinEn.

## Acquiring a Palm Pilot

Before you begin:

- The Palm Pilot is not yet added to the case
  - The examination machine is booted into Windows
  - Your EnCase application is running
1. Put the Palm Pilot or Handsprings PDA in its cradle, and attach the cradle cable to a USB or serial port on the examination machine.
  2. Turn on the PDA, then to put the PDA in console mode:
    - a. On the left side of the graffiti area, use the stylus to write a lowercase cursive "L" followed by two dots
    - b. On the right side of the graffiti area, write a "2".

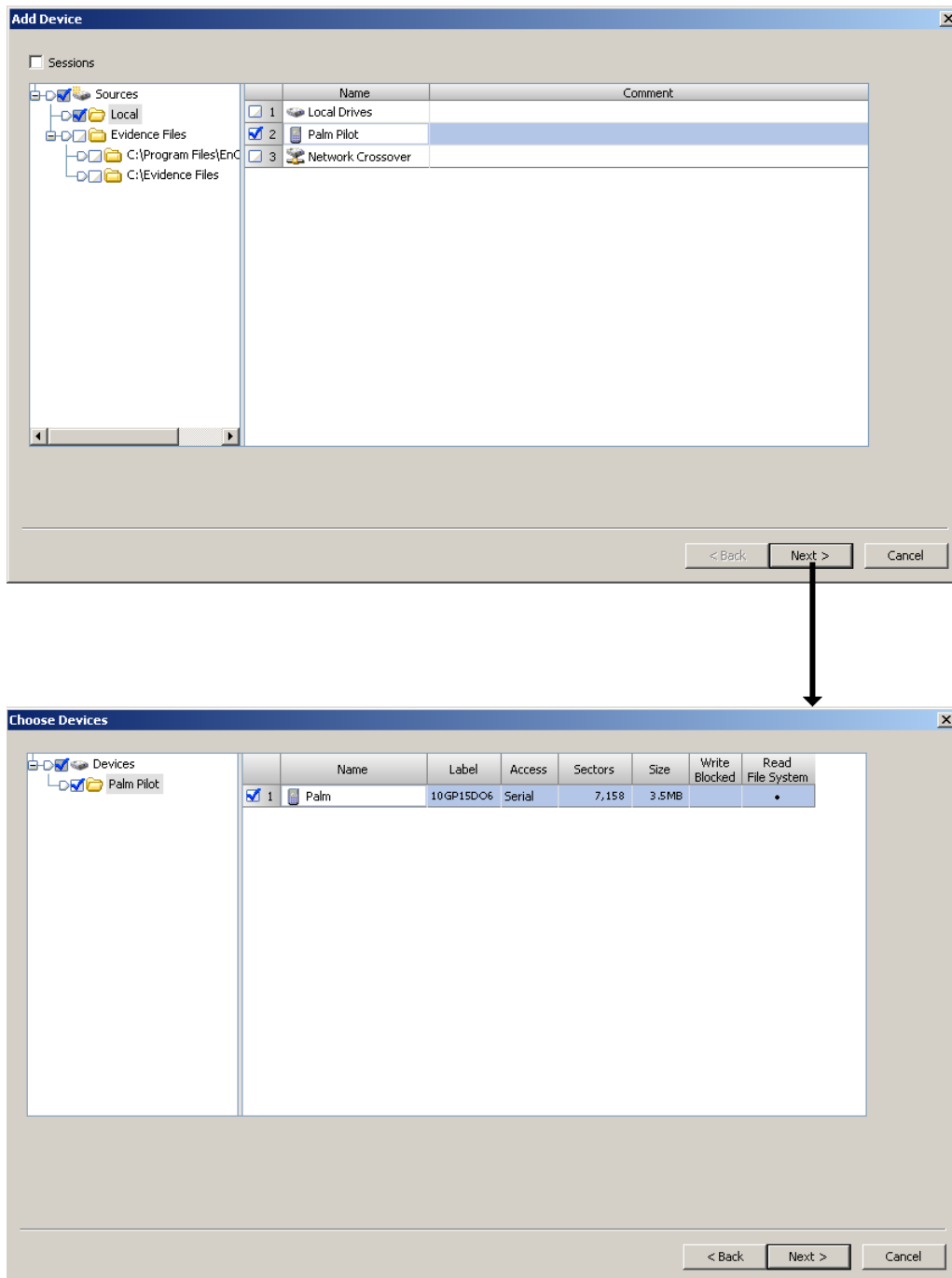
The PDA is in console mode.



On the Sources page of the Add Device Wizard:

1. In the Tree pane, click **Local**.
2. In the Table pane, click the checkbox for **Palm Pilot**.
3. If other devices are to be acquired in this acquisition continue defining devices (see Completing the Sources Page) or click **Next**.

The Choose Devices page of the Add Device Wizard displays.



4. On the Choose Devices Page, in the Table pane select the entry for the Palm Pilot device and any other devices to be acquired during this acquisition, and click **Next**.

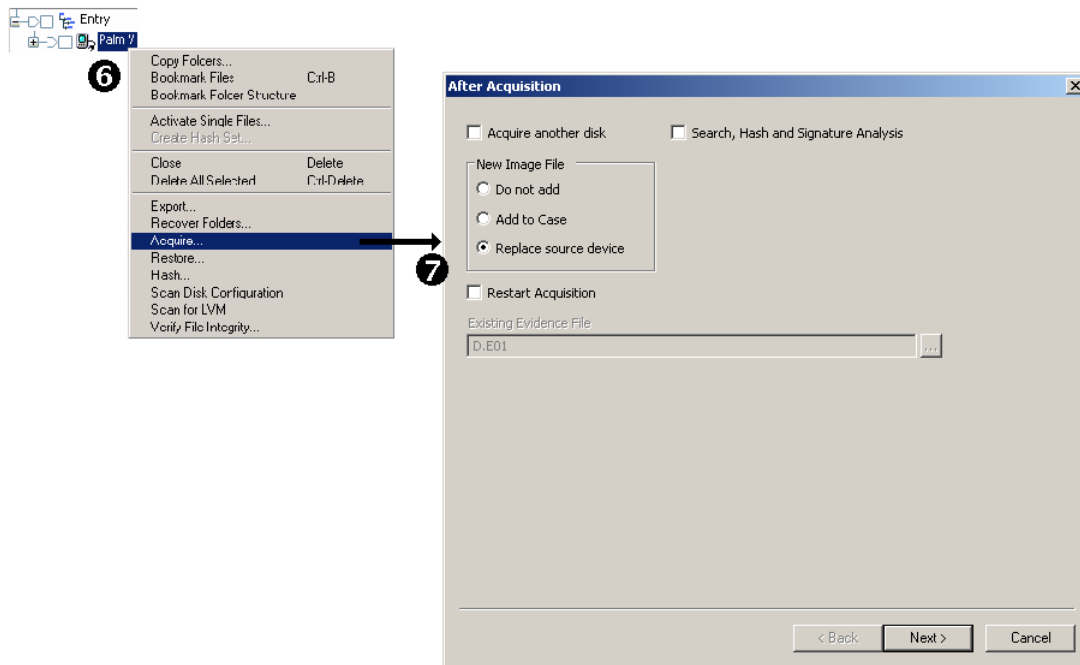
The Preview Devices page of the Add Device Wizard appears.

5. On the Preview Devices Page in the Table pane select the entry for the Palm Pilot device, and any other devices to be acquired during this acquisition, and click **Finish**.

In the **Cases > Entry > Home** tab of the main window, the Palm Pilot to be acquired appears in the Entry tree .

6. Right-click the Palm Pilot object in the Entry tree, and click **Acquire**.

The After Acquisition page of the Acquisition wizard appears.



7. Continue the acquisition from Step 1 of Specifying and Running an Acquisition

When the Acquisition Results dialog closes, the acquisition is complete.

## Leaving Console Mode

To leave console mode, you must do a soft reset on the Palm Pilot. Turning the Palm Pilot off and back on does not take it out of console mode, and leaving it in console mode causes the battery to drain faster than usual.

*To leave console mode:*

1. Locate the small hole on the back of the Palm Pilot labeled RESET.
2. Press the tip of a pen into the hole.

## Acquisition Times

Initially, previewing a serial Palm Pilot PDA may be slow because standard serial ports transfer data at a maximum speed of 115kbps. The preview and acquisition of a Palm Pilot Vx, for example, takes between 30 and 40 minutes. USB Palm Pilots will be faster: in acquisition tests, a 12MB m500 took four minutes to preview and 16 minutes to acquire. However, after the first keyword search on a previewed device, all other processes accessing the evidence file will be fast, as the entire evidence file is cached in memory.

## Acquiring Non-local Drives

The acquisition of non-local drives involves LinEn, which acquires these drives by performing a network crossover acquisition. When you use the LinEn utility to acquire a disk through a disk-to-disk acquisition, the resulting EnCase® evidence file must be added to the case using the Add Device Wizard.

## When to use a Crossover Cable

Use a crossover cable when acquiring from a laptop, RAIDs, or drives not recognized by the host machine. You can also use the crossover cable to preview.

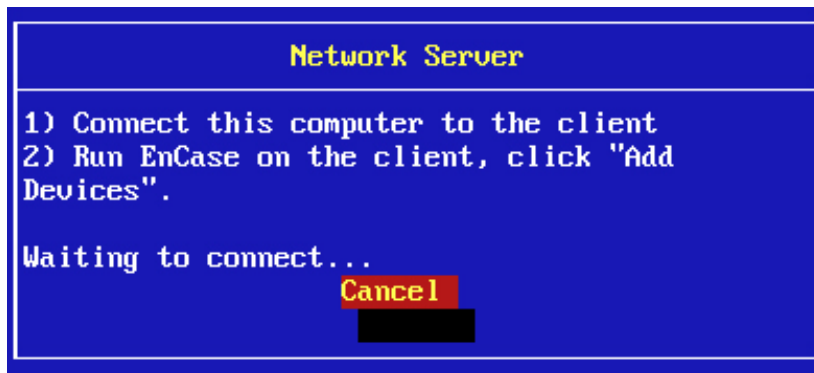
## Performing a Crossover Cable Preview or Acquisition

You have a LinEn boot disk.

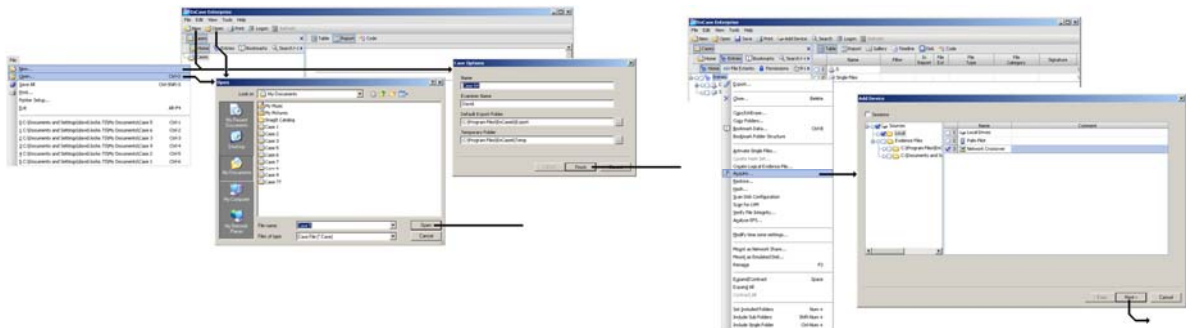
The investigator identifies the subject drive to be acquired.

1. Boot the subject machine from the LinEn boot disk.
2. Connect the forensic machine to the subject machine using a crossover cable.
3. In Linux, ensure that the subject machine has an IP address assigned and a NIC card loaded appropriately:
  - a. Type `ifconfig eth0`
  - b. If no IP address is assigned, assign one by typing `ifconfig eth0 10.0.0.1 netmask 255.0.0.0`
  - c. Check the IP address assignment again by typing `ifconfig eth0`
4. Navigate to the folder where LinEn resides and type `./linen` in the console.  
The LinEn Main Screen appears.
5. Select **Server**, and press **Enter**.

The message Waiting to connect appears.



6. On the forensic machine, specify an IP address of 10.0.0.1 for the subject machine.
7. Launch the EnCase application on the forensic machine.



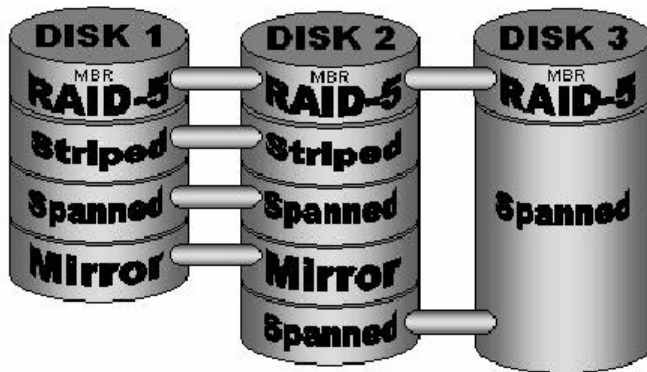
8. Create a new case, or open an existing case.
9. Right-click on the **Devices** object and click **Add Device**.
10. Select **Network Crossover**, and click **Next**.
11. Select the physical disk or logical partition to acquire or preview and click **Next**.
12. Click **Finish**.

The contents of the selected device reached through the network crossover connection are previewed. To acquire the content, perform an acquisition (see Specifying and Running an Acquisition).

## Acquiring Disk Configurations

Guidance Software uses the term *disk configuration* instead of RAID. A software disk configuration is controlled by the operating system software, whereas a controller card controls a hardware disk configuration. In a software disk configuration, information pertinent to the layout of the partitions across the disks is located in the registry or at the end of the disk, depending on the operating system; in a hardware disk configuration, it is stored in the BIOS of the controller card. With each of these methods, 6 disk configuration types can be created:

- Spanned
- Mirrored
- Striped
- RAID-5
- RAID-10
- Basic



## Software RAID

EnCase applications support these software RAIDs:

- Window NT, see Windows NT - Software Disk Configuration
- Windows 2000, see Dynamic Disks
- Windows XP, see Dynamic Disks
- Windows 2003 Servers, see Dynamic Disks

## Windows NT - Software Disk Configurations

In a Windows NT file system, you can use the operating system to create different types of disk configurations across multiple drives. The possible disk configurations are

- Spanned
- Mirrored
- Striped
- RAID 5
- Basic

The information detailing the types of partitions and the specific layout across multiple disks is contained in the registry of the operating system. EnCase applications can read this registry information and resolve the configuration based on the key. The application can then virtually mount the software disk configuration within the EnCase case.

There are two ways to obtain the registry key:

- Acquiring the drive
- Backing up the drive

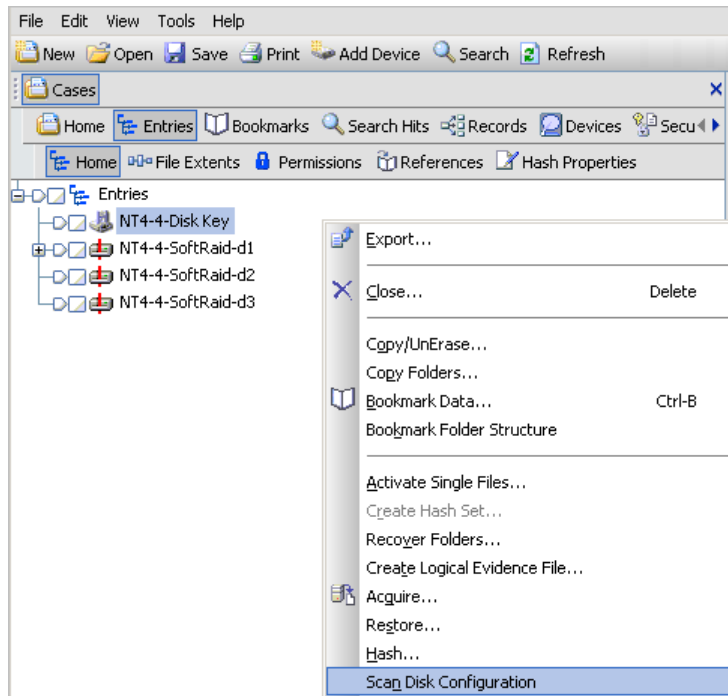
Acquire the drive containing the operating system. It is likely that this drive is part of the disk configuration set, but in the event it is not—such as the disk configuration being used for storage purposes only—acquire the OS drive and add it to the case along with the disk configuration set drives.

To make a backup disk on the subject machine, use Windows Disk Manager and select **Backup** from the **Partition** option.

This creates a backup disk of the disk configuration information, placing the backup on a floppy disk. You can then copy the file into your EnCase application using the **Single Files** option, or acquire the floppy disk and add it to the case. The case must have the disk configuration set drives added to it as well. This situation only works if working with a restored clone of a subject computer. It is also possible a registry backup disk is at the location.

Right-click the evidence file that contains the key and select Scan Disk Configuration. At this point, the application attempts to build the virtual devices using information from the registry key.





## Dynamic Disk

Dynamic Disk is a disk configuration available in Windows 2000, Windows XP and Windows 2003 Server. The information pertinent to building the configuration resides at the end of the disk rather than in a registry key. Therefore, each physical disk in this configuration contains the information necessary to reconstruct the original setup. EnCase applications read the Dynamic Disk partition structure and resolve the configurations based on the information extracted.

To rebuild a Dynamic Disk configuration, add the physical devices involved in the set to the case and, from the Cases tab, right-click on any one of the devices and choose **Scan Disk Configuration**.

If the resulting disk configurations seem incorrect, you can manually edit them via the **Edit** command in the **Devices** tab.

## Hardware Disk Configuration

Hardware disk configurations can be acquired

- As one drive
- As separate drives

Both Raid-5 and Raid-10 can be acquired.

### Disk Configuration Set Acquired as One Drive

Unlike software disk configurations, those controlled by hardware contain necessary configuration information in the card's BIOS. Because the disk configuration is controlled by hardware, EnCase cannot reconstruct the configurations from the physical disks. However, since the pertinent information to rebuild the set is contained within the controller, the computer (with the controller card) actually sees a hardware disk configuration as one (virtual) drive, regardless of whether the set consists of two or more drives. Therefore, if the investigator acquires the set in its native environment, the disk configuration can be acquired as one drive, which is the easiest option. The best method for performing such an acquisition is to conduct a crossover network cable acquisition.

---

**Note:** The LinEn boot disc for the subject computer needs to have Linux drivers for that particular RAID controller card.

---

To acquire the set:

1. Keep the disk configuration intact in its native environment.
2. Boot the subject computer with an EnCase Network Boot Disk.
3. Launch the LinEn utility.

---

**Note:** The BIOS interprets the disk configuration as one drive, so EnCase applications will as well. The investigator sees the disk configuration as one drive.

---

4. Acquire the disk configuration as you would normally acquire a single hard drive depending on the means of acquisition. Parallel port, crossover network cable, or drive-to-drive acquisition is straightforward, as long as the set is acquired as one drive.

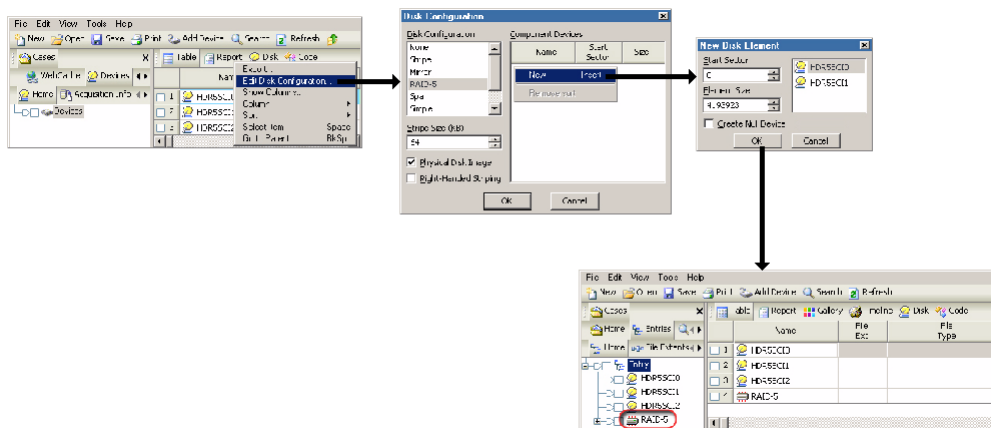
If the physical drives were acquired separately, or could not be acquired in the native environment, EnCase applications can edit the hardware set manually.

## Disk Configurations Acquired as Separate Drives

Sometimes acquiring the hardware disk configuration as one drive is not possible, or the method of assembling a software disk configuration seems incorrect. To edit a disk configuration, several items of information are required:

- the stripe-size
- start sector
- length per physical disk
- whether the striping is right handed or not

You can collect this data from the BIOS of the controller card for a hardware set, or from the registry for software sets.



When a RAID-5 consists of three or more disks and one disk is missing or bad, the application can still rebuild the virtual disk using parity information from the other disks in the configuration, which is detected automatically during the reconstruction of hardware disk configurations using the **Scan Disk Configuration** command.

When rebuilding a RAID from the first two disks, results from validating parity are meaningless, because you create the parity to build the missing disk.

To acquire a disk configuration set as one disk:

1. Add the evidence files to one case.
2. **View > Cases Subtabs > Devices.**
3. Right-click any evidence file row and select **Edit Disk Configuration**.
4. The Disk Configuration dialog appears.

5. In Disk Configuration, right-click on the appropriate disk configuration, then click **New**.
6. Enter the start sector and size of the selected disk configuration, and then click **OK**.

## Validating Parity on a RAID-5

The Validate Parity command checks the parity of the physical disks used to assemble the RAID-5. Thus, if the RAID-5 was rebuilt with a missing disk, this feature will not work.

To check the parity:

1. From the Cases tab, right-click the RAID 5 volume icon, and then click **Validate Parity**.
2. The validation process status displays in the Thread Status line at the bottom right of the EnCase main window.

## RAID-10

RAID-10 arrays require at least 4 drives, implemented as a striped array of RAID-1 arrays.

## Acquiring Virtual PC Images

With Microsoft Virtual PC 2004 you can run multiple PC- based operating systems simultaneously on one workstation. Users save images of these virtual PCs in a fashion similar to VMware. EnCase applications treat Microsoft Virtual PC 2004 images as devices to be submitted to the same investigation as physical devices. Virtual PC can create flat and sparse files, both of which are supported transparently by EnCase applications.

Add Virtual PC files via the Add Device Wizard. In the Wizard, navigate to the folder containing Virtual PC files (\*.vhd) and add them as an EnCase evidence file.

## CD-DVD Inspector File Support

EnCase applications support viewing files created using CD/DVD Inspector, a third-party product. Treat these files as single files when adding them, as zip files, or as composite files when using the file viewer. Drag single files into the application.

## Acquiring SlySoft CloneCD Images

You can add raw CD-ROM images created using SlySoft CloneCD to a case. When adding these images, you can specify the pre-sector bytes, post-sector bytes and start byte of the image.

## Acquiring a DriveSpace Volume

DriveSpace volumes are only recognized as such after they are acquired and mounted into a case. On the storage computer, mount the DriveSpace file as a volume, and then acquire it again to see the directory structure and files.

### *To acquire a DriveSpace volume*

1. A FAT16 partition must exist on the forensic PC where you will Copy/Unerase the DriveSpace volume. A FAT16 partition can only be created with a FAT16 OS (such as Windows 95).
2. Run FDISK to create a partition, then exit, reboot, and format the FAT16 partition using format.exe.
3. Image the DriveSpace volume.
4. Add the evidence file to a new case and search for a file named DBLSPACE.000 or DRVSPACE.000.
5. Right-click the file and copy/unerase it to the FAT16 partition on the storage computer.
6. In Windows 98, click **Start** and select **All Programs Accessories > System Tools DriveSpace**.
7. Launch DriveSpace.
8. Select the FAT16 partition containing the compressed “.000” file.
9. Select **Advance Mount**.
10. Select **DRVSPACE.000** and then click **OK**, noting the drive letter assigned to it. The Compressed Volume File (.000) from the previous drive is now seen as folders and files in a new logical volume.
11. Acquire this new volume.
12. Create the evidence file and add to your case.

You can now view the compressed drive.

## Acquiring Firefox Cache in Records

This feature parses Mozilla Firefox cache data. The parser correctly extracts all available information by reading map files that contain information about a cache entry and where it is located.

When you select Search for Internet History from the Search dialog, the EnCase® program searches for specific files and attempts to parse them as Mozilla Firefox cache files. When the search is complete, these columns are shown in the Table pane:

- Name
- Filter
- In Report
- Search Hits
- Additional Fields
- Message Size
- Creation Time
- Profile Name
- URL Name
- URL Host
- Browser Cache Type
- Browser Type
- Last Modification Time
- Message Code Page
- Last Access Time
- Expiration
- Visit Count
- Server Modified

## Reacquiring Evidence

When you have a raw evidence file which originated outside an EnCase application, reacquiring it results in the creation of an EnCase evidence file containing the content of the raw evidence file.

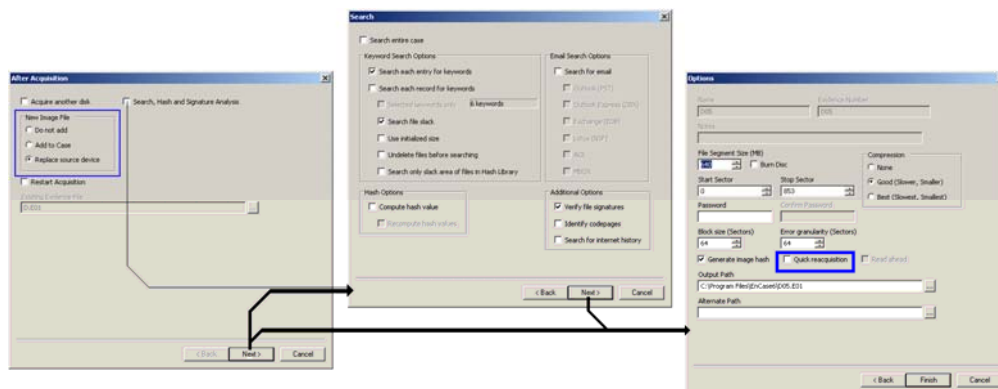
You can move EnCase evidence files into a case even if they were acquired elsewhere. This does not require a reacquisition. Just drag the files from Windows Explorer and drop them on the Sessions Sources page of the Add Device Wizard.

You may also want to reacquire an existing EnCase evidence file to change the compression settings or the file segment size.

## Reacquiring an Evidence File

Before you begin:

- Your EnCase application is open
- The file to be reacquired is included in the case
- The case has been opened



*To reacquire an evidence file:*

1. In the Tree pane, click **Cases > Entries > Home**.  
The Entries tree appears in the Tree pane.
2. Right-click the device to be reacquired, and click **Acquire**.  
The After Acquisition page of the Acquisition wizard appears.
3. Perform the acquisition (see Specifying and Running an Acquisition).
4. Pay particular attention to the disposition of the file:
  - a. Use the **New Image File** controls on the After Acquisition page.

- b. Click **Quick Reacquisition** on the Options page of the Wizard.

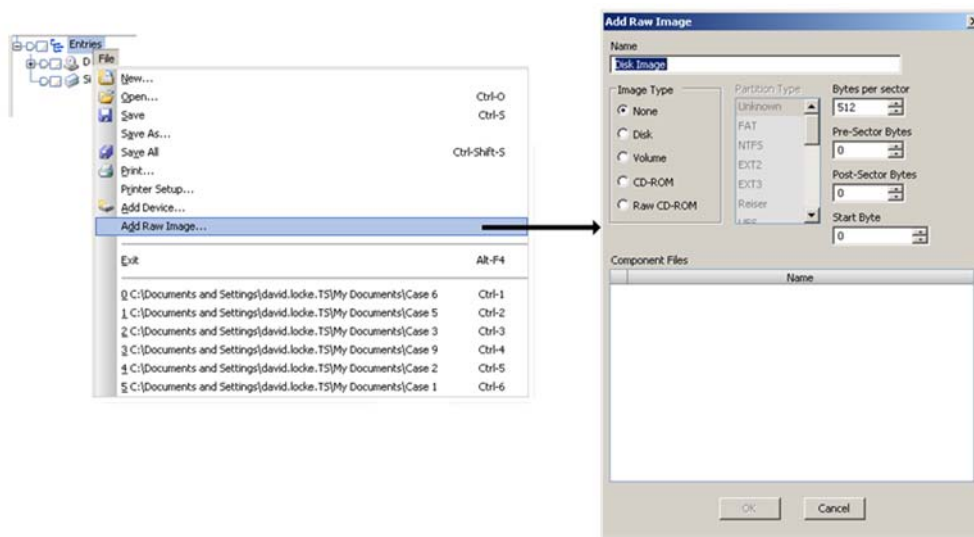
The evidence file is reacquired.

## Adding Raw Evidence Files

Reacquiring a raw evidence file embeds the file containing the image of the contents of a device with case metadata and, optionally, the hash value of that image.

Before you begin:

- You have a raw image file that can be accessed by the forensic machine
- A case is open



*To acquire a raw evidence file:*

1. In the Tree pane, click **Cases > Entries > Home**.  
The Entries tree appears in the Tree pane.
2. Click **File > Add Raw Image**.  
The Add Raw Image dialog appears.
3. Drag and drop the raw images to be acquired  
The raw images to be added are listed in the Component Files list.
4. Accept the defaults in the Add Raw Image dialog or change them as desired, then click **OK**.

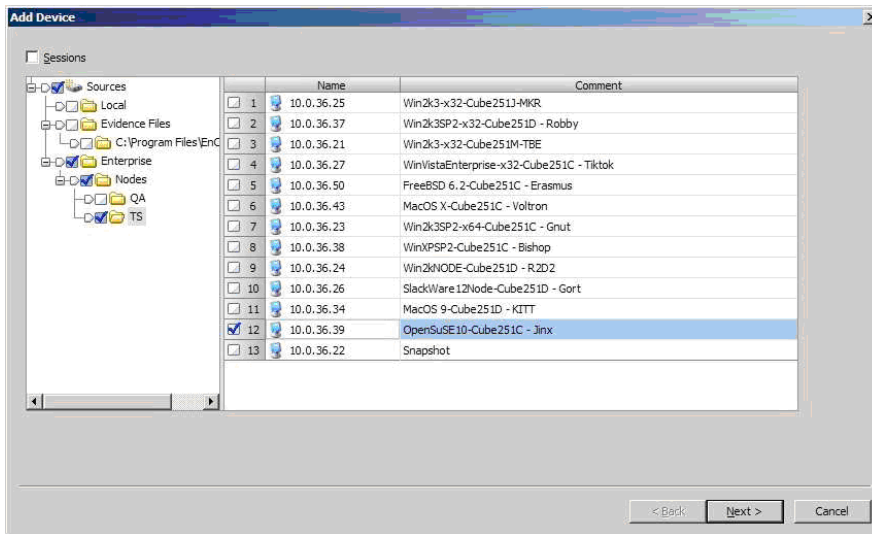
A Disk Image object appears in the Entries tree, which is on the **Cases > Entries > Home** tree pane.



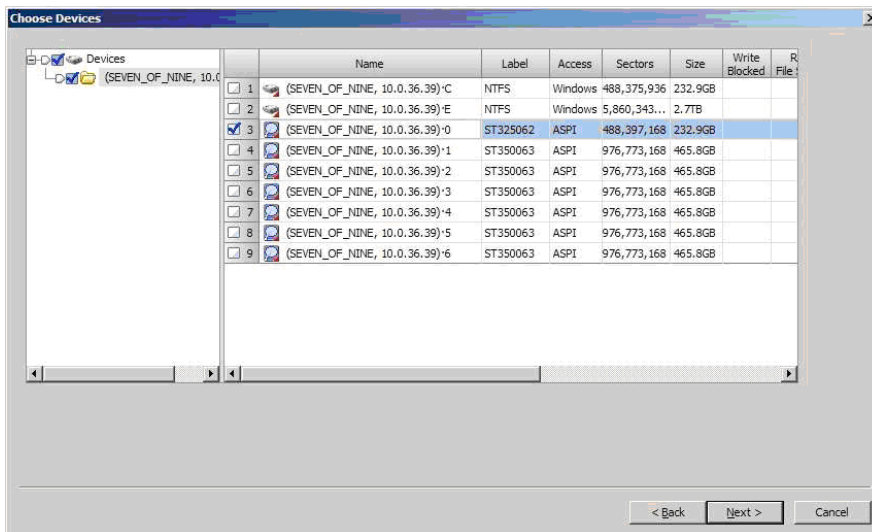
## Remote Acquisition

Setting up the remote acquisition Examiner side:

1. Start by adding the machine you want to acquire just as you would any other Enterprise node.

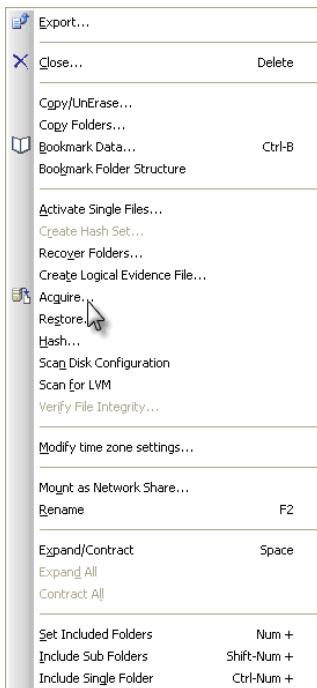


2. Click Next.
3. After you choose the machine, select the devices you want to acquire.

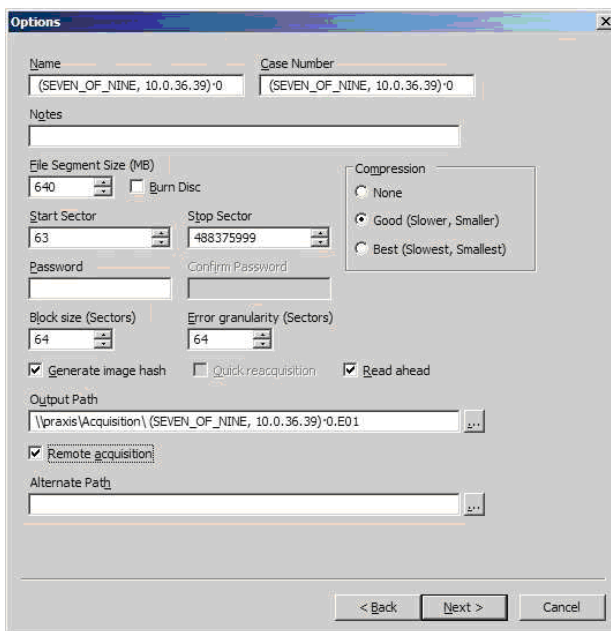


4. Click Next.

5. Right-click the device you want to acquire, then click **Acquire**.

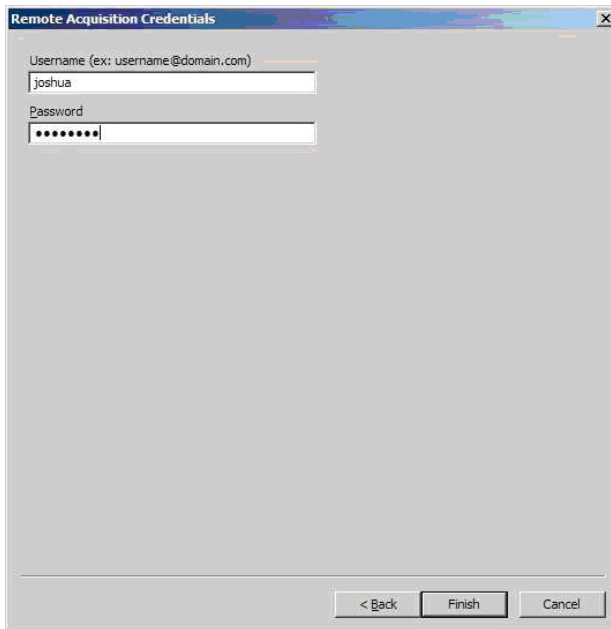


6. Click **Next** until you reach the Options dialog.

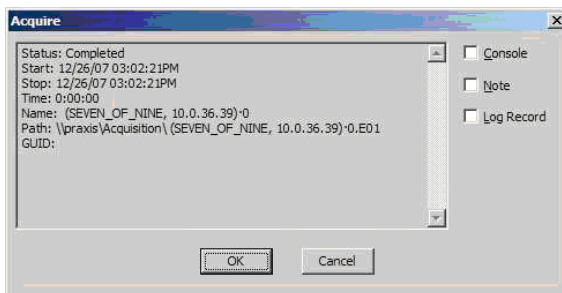


7. Enter the remote acquisition information, including a valid **Output Path**.
8. Click the **Remote acquisition** check box.
9. Click **Next**.

10. Enter a Username and Password for the remote share.



11. Click **Finish**. The Acquire dialog displays:

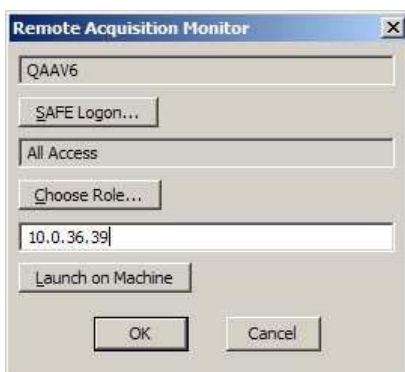


12. Click **OK**.

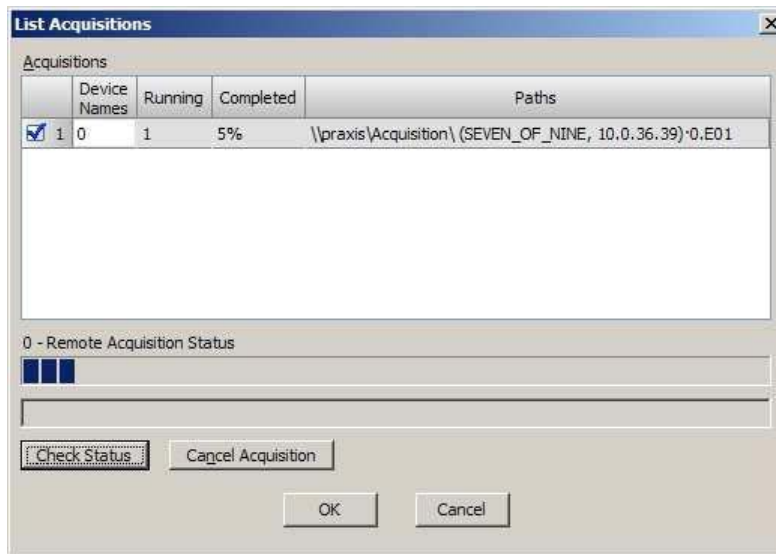
## Remote Acquisition Monitor

Use the Remote Acquisition Monitor to check the progress of the acquisition.

1. Double-click **Remote Acquisition Monitor** and enter the appropriate information.



2. Click **OK**.
3. The monitor connects to the machine and displays the acquisition's progress.



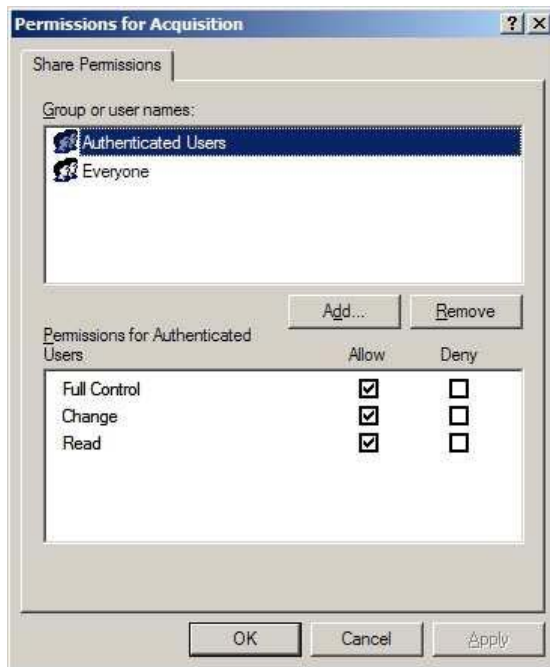
## Setting Up the Storage Machine

This is basic Windows share setup.

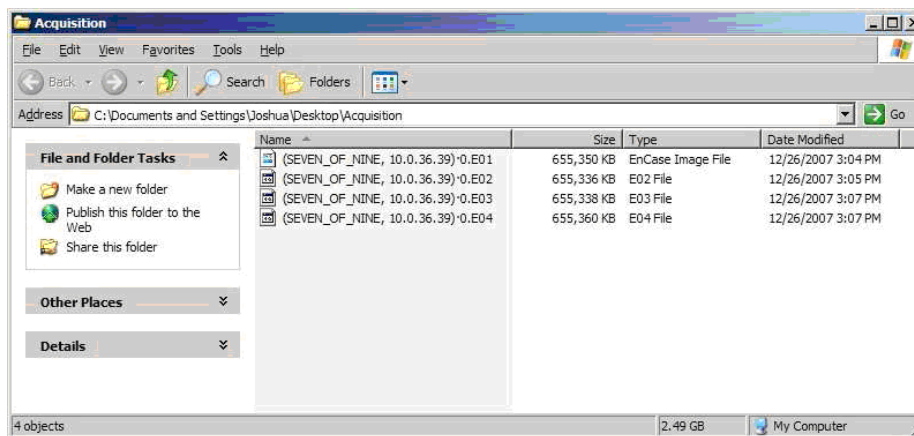
1. In the Acquisition Properties dialog, select the **Sharing** tab.



2. Click the **Share this folder** radio button and enter a Share name.
3. Click **Permissions**.
4. The Permissions for Acquisition dialog displays. These settings vary, depending on your environment.



5. Set up the permissions you want, then click **OK**.
6. The shared folder looks like this:



## Hashing

You can perform hashing before or after an acquisition, so an investigator can determine if the device should be acquired, or if the contents have changed. You must run a preview if working within the Windows version of EnCase (this is not necessary when hashing a drive using the LinEn utility).

---

Note: If you are hashing the device locally using Windows, a write blocking device, such as the FastBloc® write blocker, prevents the subject device from changing. Hashing via a crossover network cable, or locally using the LinEn utility is useful if a write blocking device is not available.

---

There are two ways to hash a drive:

- Hashing the subject drive using LinEn
- Hashing the subject drive once previewed or acquired

### Hashing the Subject Drive Using LinEn

This allows the investigator to know the hash value of the drive.

Before you begin:

- LinEn is configured as described in the setup topics
- **autofs** is disabled
- The investigator has identified the subject drive to be hashed

#### *To perform a hash using LinEn*

1. Navigate to the folder where LinEn resides and type `./linen` in the console to run LinEn.  
The LinEn Main Screen appears.
2. Select **Hash**.  
The Hash dialog appears.
3. Select a drive, then click **OK**.  
The Start Sector dialog appears.
4. Accept the default or enter the desired **Start Sector**, and then click **OK**.  
The Stop Sector dialog appears.
5. Accept the default or enter the desired **Stop Sector**, and then click **OK**.  
The Hash Results dialog appears.

6. If you want the hash result to be written to a file, click **Yes**.

If the hash value is to be saved to a file, the Save Hash Value to a File dialog appears; otherwise, the LinEn Main Screen appears.

7. Enter the path and filename of the file that will contain the hash value, and then click **OK**.

The hash value is saved and the LinEn Main Screen appears.

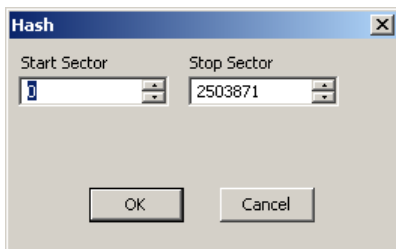
A hash value is calculated for the selected sectors of the selected file. If desired, this hash value is saved to a file.

## Hashing the Subject Drive Once Previewed or Acquired

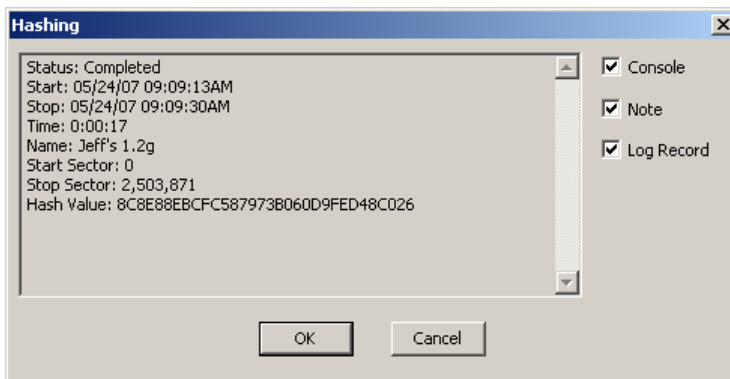
If you want to hash a device without leaving the Windows operating system, you can hash directly from EnCase.

The device must be previewed or acquired.

1. On the Entries tab on the Tree pane, right-click the device you want to hash.
2. Select **Hash**.



3. Enter the following:
  - a. Supply a **Start Sector**, or accept the default, which is the first sector of the device
  - b. Supply a **Stop Sector**, or accept the default value, which is the last sector of the device
4. Click **OK**.



5. Select one of the following output formats:
  - ☐ **Console** writes the results in the console tab
  - ☐ **Note** writes the results as a note bookmark
  - ☐ **Log Record** writes the results as a log record bookmark
6. Click **OK**.

## Logical Evidence Files

A Logical Evidence File (LEF) contains a collection of individual files typically copied from a subject computer when previewing.

As you examine digital evidence, some of the evidence is more significant to the intent of the investigation. During the analysis of the EnCase evidence file, various searches are performed to find these significant files. By copying these significant files into a logical evidence file you can access them without dealing with the large volume contained in an EnCase evidence file.

Dragging and dropping a LEF anywhere on the EnCase interface adds the LEF to the currently opened case.



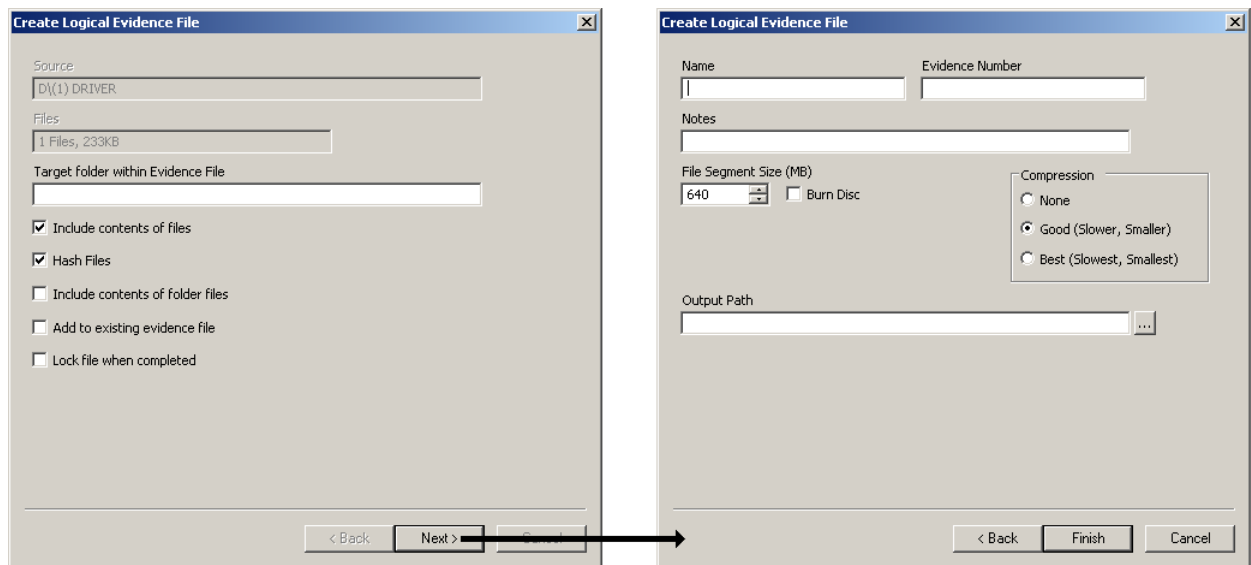
## Create Logical Evidence File Wizard

Use the Create Logical Evidence File Wizard to create logical evidence files associated with the currently opened case.

Before a logical evidence file can be created, open the case associated with it and select the associated files you want to acquire.

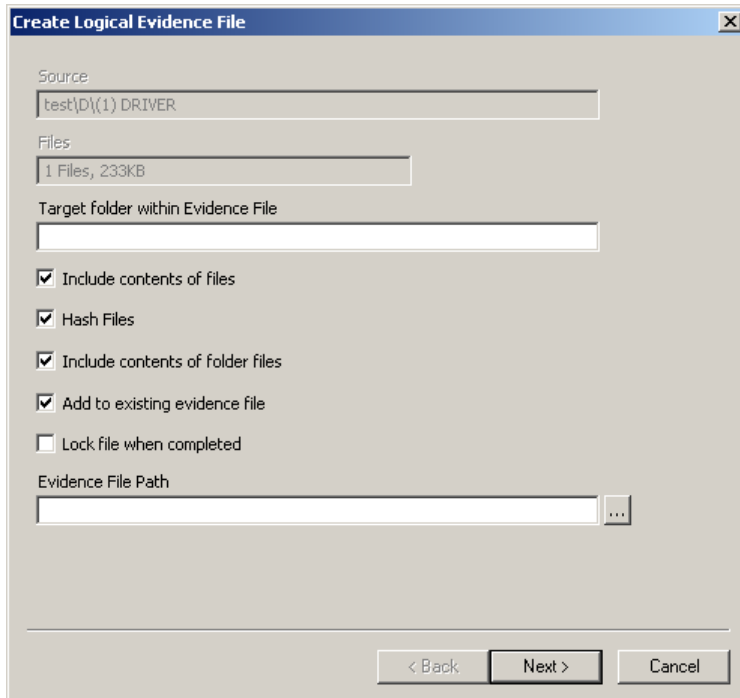
The Create Logical Evidence File wizard contains the following pages:

- Sources page
- Outputs page



## Sources Page

Use the Sources Page of the Create Logical Evidence File Wizard to specify source files that will comprise the logical evidence file being created.



The screenshot shows the 'Create Logical Evidence File' wizard, Sources page. The window has a title bar with the text 'Create Logical Evidence File' and a close button. The main area contains several input fields and checkboxes. The 'Source' field is a text box containing 'test\D\{1} DRIVER'. The 'Files' field is a text box containing '1 Files, 233KB'. The 'Target folder within Evidence File' field is an empty text box. Below these fields are five checkboxes: 'Include contents of files' (checked), 'Hash Files' (checked), 'Include contents of folder files' (checked), 'Add to existing evidence file' (checked), and 'Lock file when completed' (unchecked). Below the checkboxes is the 'Evidence File Path' field, which is an empty text box with a browse button (three dots) to its right. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

**Source** is the name of the parent device containing the file or files to include in the logical evidence file.

**Files** contains the number of files and the total size of the file or files to include in the logical evidence file.

**Target folder within Evidence File** is the name of the folder containing the files that comprise the logical evidence file.

**Include contents of files:** if disabled, only the filename is known to the logical evidence file, and when the logical evidence file is opened, no data displays in the View pane.

**Hash Files** determines whether the files comprising the logical evidence file are hashed as they are put into the logical evidence file.

**Add to existing evidence file** determines whether the files comprising the logical evidence file are added to an existing evidence file. When this control is enabled, **Evidence File Path** appears.

**Lock file when completed** determines whether the logical evidence file is locked after creation.

**Evidence File Path** contains the path and filename of the logical evidence file, where the selected files will be added.

## The Outputs Page of the Create Logical Evidence File

Use the Outputs page of the Create Logical Evidence File wizard to specify the metadata and output attributes of the logical evidence file to be created.

The screenshot shows a Windows-style dialog box titled "Create Logical Evidence File". The dialog has a light gray background and a blue title bar with a close button (X) in the top right corner. The main area contains several input fields and controls:

- Name**: A text input field.
- Evidence Number**: A text input field.
- Notes**: A multi-line text area.
- File Segment Size (MB)**: A spinner control set to "640".
- Burn Disc**: A checkbox that is currently unchecked.
- Compression**: A group box containing three radio buttons:
  - ☐ None
  - ☒ Good (Slower, Smaller)
  - ☐ Best (Slowest, Smallest)
- Output Path**: A text input field with a browse button (three dots) to its right.

At the bottom of the dialog, there are three buttons: "< Back", "Finish", and "Cancel". The "Finish" button is highlighted with a black border.

**Name** contains the name of the logical evidence file to be created.

**Evidence Number** contains the investigator's evidence number for the logical evidence file to be created.

**File Segment Size** contains the file segment size of the logical evidence file to be created.

**Compression** contains controls that determine the compression used when creating the logical evidence file.

**None** means no compression is used when creating the logical evidence file.

**Good:** good compression is used to create a logical evidence file that is smaller than when no compression is used, but larger than when best compression is used.

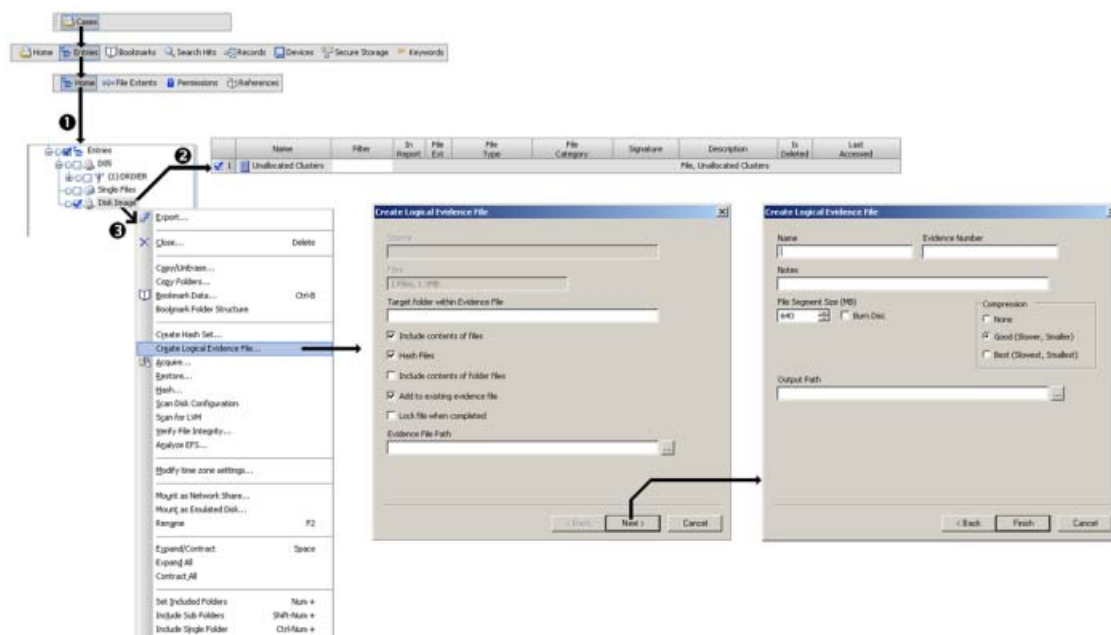
**Best:** best compression is used to create a logical evidence file that is smaller than one created with good compression.

**Output Path** contains the path and filename of the logical evidence file to be created.

## Creating a Logical Evidence File

Before you begin:

Open the case associated with the logical evidence file to be created in EnCase.



*To create a logical evidence file.*

1. In the Tree pane, click **Cases > Entries > Home**.

The Entries tree appears in the Tree pane.

2. Select the files and folders to be associated with the logical evidence file.

3. Right click the parent object on the Entry tree, and click **Create Logical Evidence File**.

The Sources page of the Create Logical Evidence File wizard appears.

4. Accept the default settings or enter desired values, and then click **Next**.

The Outputs page of the Create Logical Evidence File wizard appears.

5. Enter the appropriate values, and enter or browse to the path and filename of the logical evidence file to be created.

6. Click **Next**.

The results dialog appears with a status of complete.

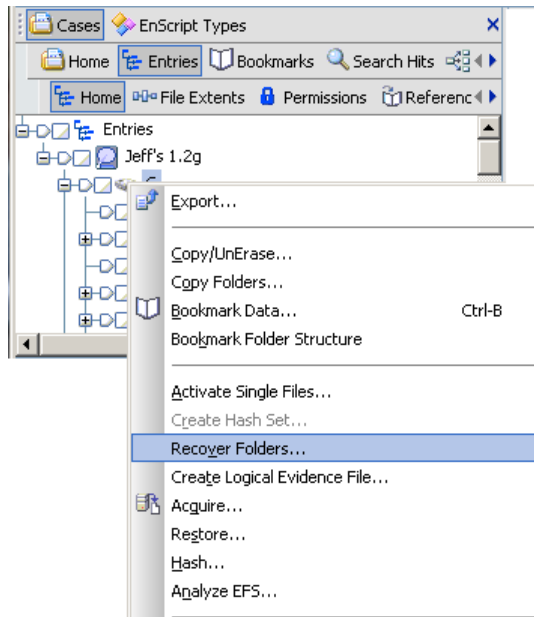
## Recovering Folders

The following types of folders can be recovered:

- Folders on FAT volumes, as described in Recovering Folders on FAT Volumes
- NTFS folders, as described in Recovering NTFS Folders
- UFS and EXT2/3 partitions, as described in Recovering UFS and EXT2/3 Volumes

## Recover Folders on FAT Volumes

After adding an evidence file to a case, run Recover Folders on all FAT partitions by right clicking on each device and selecting it. This command searches through the unallocated clusters of a specific FAT partition for the “dot, double-dot” signature of a deleted folder; when the signature matches, EnCase applications can rebuild files and folders that were within that deleted folder.



Note that in the figure, the C:\ drive device is selected in the background display.

## Recovering NTFS Folders

EnCase applications can recover NTFS files and folders from Unallocated Clusters and continue to parse through the current Master File Table (MFT) records for files without parent folders. This is particularly useful when a drive has been reformatted or the MFT is corrupted. Recovered files are placed in the gray Recovered Folders virtual folder in the root of the NTFS partition.

To recover folders on an NTFS partition:

1. Right-click on the volume and select **Recover Folders**.
2. The Recover Folders message box opens to confirm that you want to scan the volume for folders.
3. Click **OK** to begin the search for NTFS folders, or **Cancel** to cancel the request.

4. The application begins searching for MFT records in the Unallocated Clusters. In the bottom right-hand corner a progress bar indicates the number of MFT records found and the approximate time required to complete the search.
5. After the application locates the MFT records in the Unallocated Clusters, a prompt appears showing the number of entries found. Duplicate or false hits are parsed, so the number of entries that appears in the prompt may be lower than reported during the recovery.
6. Click **OK**.
7. The application resolves the recovered MFT records to data on the volume, and attempts to rebuild the folder structure with children files and folders under parent folders. This process can take a long time; however, the results greatly benefit examinations of NTFS volumes.

Since rebuilding the folder structure can take a long time, you can opt to have faster access to the recovered files. If the recovered MFT entries in the unallocated space are NTFS4, you can choose to:

- process the entries for parent/child relationships, or
- place all recovered entries into the Recovered Files folder immediately with no folder structure.

This dialog box shows the number of passes required to sort the entries. This number may be large, but most passes process instantly. The length of time required to process a given group depends only on the number of records within that group.

This change does not affect NTFS5 recovered entries. These entries are processed quickly, as before. If you choose to process the entries for the folder structure, the progress bar indicates which pass is currently running. The recovered folder structure is placed under the virtual Recovered Files folder.

## Recovering UFS and EXT2/3 Partitions

EnCase applications use a different method for recovering deleted files and folders that have no parent in UFS and EXT2/3 partitions. When you preview a computer or add an evidence file containing one of these partitions to your case, a gray folder called **Lost Files** is automatically added to the tree in the Entries tab as a child of each partition.

In the Master File Table (MFT ) in NTFS, all files and folders are marked as a folder or file and as belonging to a parent. The files within a folder are that folder's children. If you first delete the files, then delete the folder, and then create a new folder, the originally deleted files can be lost.

The new folder's entry in the MFT overwrites the deleted folder's entry. The original parent folder and its entry in the MFT are overwritten and gone. Its children, however, were not overwritten and their entries are still in the MFT. As with NTFS, with UFS and EXT2/3 partitions, the application parses the MFT and finds those files that are still listed, but have no parent directory. All of these files are recovered and placed into the gray **Lost Files** folder.

## Recovering Folders from a Formatted Drive

If the evidence file shows a logical volume but has no directory structure, the hard drive has probably been formatted. If this is a FAT-based system, EnCase applications can recover the original directory structure. Right-click on each logical volume and choose **Recover Folders**. This searches through the drive and recovers folders, subfolders and files from within those folders if the information is still available.

You may occasionally encounter a device containing a file system unsupported by EnCase. When this occurs, the Entries tree displays the device icon, but the Entries table only lists Unallocated Clusters. Although there is no way to view file structure, it may be possible to run text searches through the Unallocated Clusters.

## Recovering Partitions

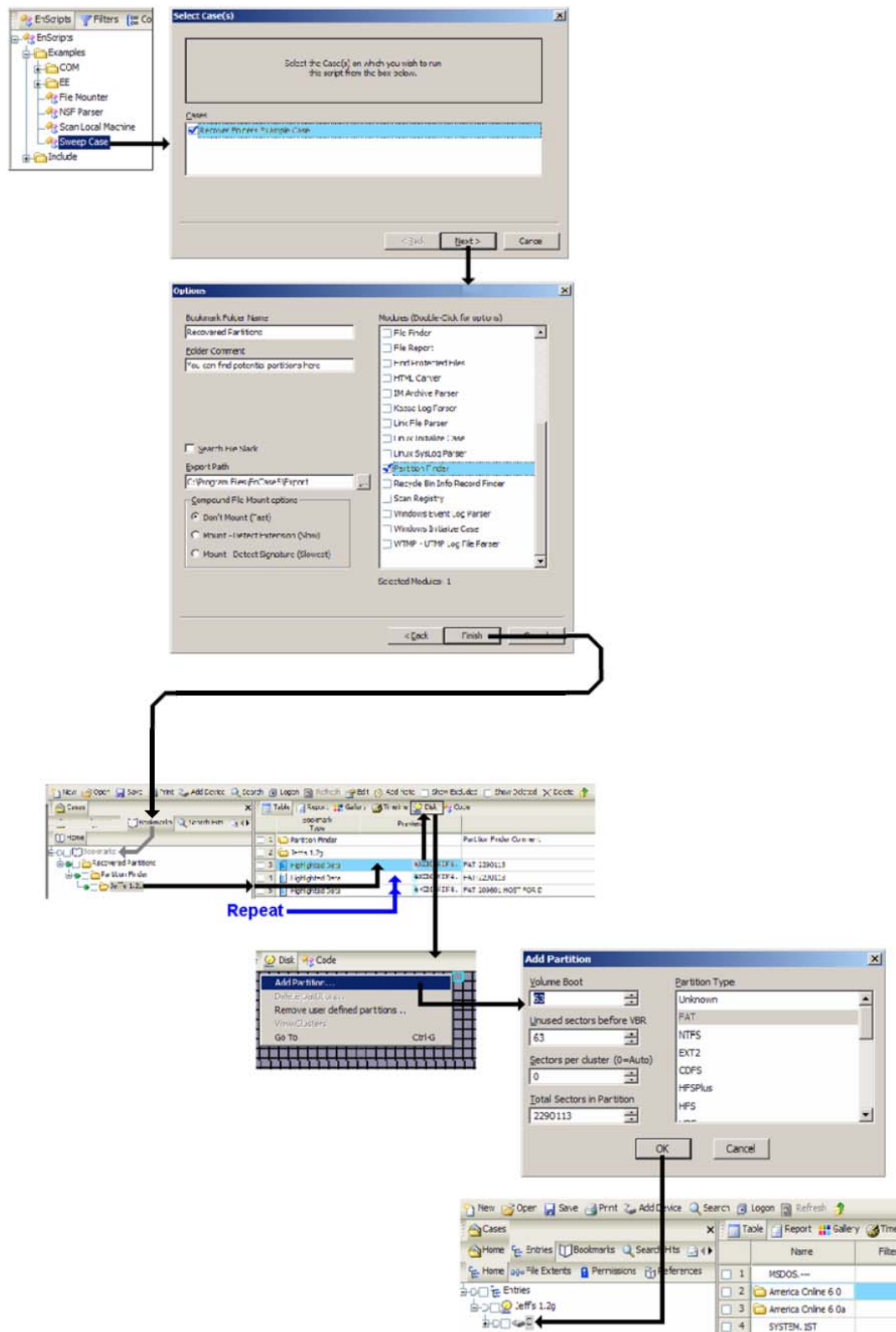
Occasionally a device is formatted or even FDISKed in an attempt to destroy evidence. Formatting and FDISKing a hard drive does not actually delete data. Formatting deletes the structure indicating where the folders and files are on the disk. FDISKing a drive deletes a drive's partition information. EnCase applications can rebuild both partition information and directory and folder structure.



## Adding Partitions

A formatted hard drive or FDISK hard drive should be acquired using normal procedures. When these evidence files are added to a case

- A formatted drive displays logical volumes within EnCase, but each volume has only an Unallocated Clusters entry in the table.
- An FDISK hard drive will not show logical volume information. The entire drive is displayed as Unused Disk Area in the table



To restructure these portions of the disk:

1. In the filter pane, expand **EnScripts > Examples**.
2. Double-click **Case Processor**.
3. Check the case you are working on and click **Next**.
4. Enter a **Bookmark Folder** name and optionally, a **Folder Comment**.
5. Check the **Partition Finder Module** in the Modules list.
6. Click **Finish**. The EnScript program runs.
7. When the EnScript program finishes, click **Bookmarks** in the Tree pane.
8. In the tree, click **Set Included** to show all the bookmarks the EnScript program has found. Note the partition type and size in the comment.
9. Highlight the entry in the Table pane, and then select **Disk**.
10. In the Disk tab, the cursor appears on the bookmarked sector. Right-click and select **Add Partition**. The Add Partition screen detects the sectors and partition type automatically, populating the fields.
11. Click **OK** to restore the partition.
12. To see the contents of the partition you just added, click **Entries** in the Tree pane. The new partition appears below the device the Sweep Case EnScript program was run against.
13. If the drive had multiple partitions, click **Bookmarks** in the Tree pane, then repeat the process from step 9.

## Deleting Partitions

If a partition was created at the wrong sector, you must delete the entry for that partition at the sector at which it was created on the evidence file image of the hard drive.

### *To delete a partition*

1. On the Disk tab of the Table pane, navigate to the volume boot record entry, as indicated by a pink block.
2. Right-click and select **Delete Partition**.
3. Click **Yes** to confirm the removal of the partition.

The row in the Table view now contains an entry for Unused Disk Space instead of the now deleted partition.

## Restoring Evidence

EnCase applications allow an investigator to restore evidence files to prepared media. Restoring evidence files to media theoretically permits the investigator to boot the restored media and view the subject's computing environment without altering the original evidence. Restoring media, however, can be challenging. Read this chapter carefully before attempting a restore.

DO NOT boot up the Subject's drive. Do not boot up your forensic hard drive with the Subject drive attached. There is no need to touch the original media at all. Remember, *it is still evidence*.

## Physical vs. Logical Restoration

EnCase allows the investigator to restore either a logical volume or a physical drive. A logical volume is a volume that does not contain a Master Boot Record (MBR) or the Unused Disk Space. A physical volume contains the Master Boot Record and Unused Disk Space. Unused Disk Space, however, is typically not accessible to the user.

Most often, when complying with discovery issues, one must perform a physical restore, not a logical one. Logical restores are less desirable as they cannot be verified as an exact copy of the subject media. When a drive is restored for the purposes of booting the subject machine, a physical restore is the correct choice.

Whether restoring a drive physically or logically, restore the evidence files to a drive *slightly* larger in capacity than the original Subject hard drive. For example, if restoring a 2-gig hard drive image, restore the image to a 2- to 4-gig hard drive. Restoring media to a drive that is substantially bigger than the subject media can prevent the restored clone from booting at all, possibly defeating the purpose of the restore.

## Preparing the Target Media

Preparation of the target media where the image is going to be restored is essential for a forensically sound restore.

- The target media must be wiped.
- For logical restores, the target media must be FDISKed.
- For logical restores, the target media must be partitioned and formatted with the same file-type system as the volume to be restored (e.g., FAT32 to FAT32, NTFS to NTFS, etc.).
- For physical restores, do not FDISK, partition, or format the hard drive. Instead, start your EnCase application and restore the image physically to the target media.

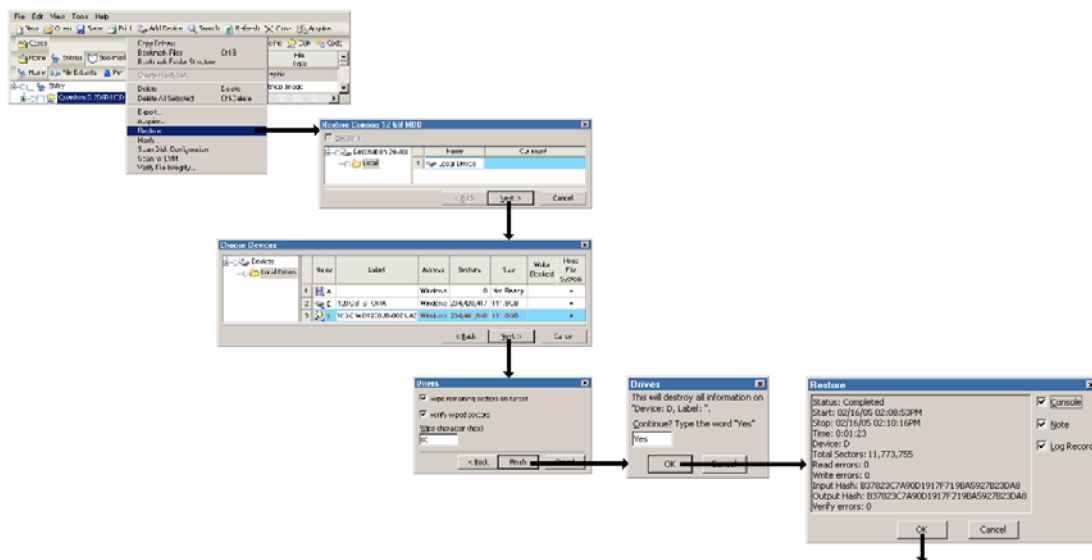
## Physical Restore

Restoring a physical drive means that the application will copy everything, sector-by-sector, to the prepared target drive, thereby creating an exact copy of the subject drive. The target drive should be larger than the subject hard drive. When the restore completes, it provides hash values verifying that the lab drive is an exact copy of the subject drive. If a separate, independent MD5 hash of the lab drive is run, be certain to choose to compute the hash over only the exact number of sectors included on the suspect's drive so that the MD5 hash will be accurate.

Drive 0 cannot be restored to. If the prepared target media is Drive 0, another drive must be added to the system, as a master, to store the restored image.

Restored sectors can also be verified to confirm that there is indeed a sector-by-sector copy of the original subject media

Sometimes the **Convert Drive Geometry** setting is available. This is entirely dependent on the drive geometry of the original drive in comparison to the restore drive. Every drive is defined by specific Cylinders- Heads-Sectors (CHS) drive geometry information. If the Heads and Sectors of the original drive imaged are identical to the target restore drive, then the drives are of the same type and the Convert Drive Geometry setting is not available. If the source and target drives are of different types (for example, the heads-sectors settings are different), then the **Convert Drive Geometry** is available.



*To restore a physical hard drive:*

1. Install a sterile, unpartitioned, unformatted restoration drive to your forensic machine, using a connection other than IDE 0. EnCase applications cannot restore a physical drive to IDE 0. Ensure that the intended restoration drive is at least as large as (but preferably larger than) the original from which the image was taken so that the restored data will never overwrite all sectors on the target hard drive. EnCase applications can wipe the remaining sectors of the target hard drive after the actual data from the evidence file is restored. Wiping remaining sectors is recommended.
2. Look at the acquired drive in the Report pane and note the precise physical drive geometry of the forensic image you are restoring from, including Cylinders, Heads and Sectors. Note the acquisition hash for later comparison on the restored drive.
3. On the Entries tree, on the Tree pane, right-click on the physical disk you wish to use as the source and select **Restore**.
4. Select the destination drive from the list of possible destination devices, and click **Next**.
5. Select the drive to restore the image to and click **Next**.
6. If it is displayed, select **Convert Drive Geometry**, and then click **Finish**.
7. To confirm the restore to the designated drive, type **Yes** in **Continue**, and then click **Yes** to start the physical restore.

When the restore is finished, a verification message displays information such as any read or write errors and the hash values for both the evidence file and the restored drive. The hash values should match. If the hash values from the restore do not match, restore the evidence file again. It might be necessary to swap the target media for correct results.

8. When the drive is restored, physically pull the power cord from the computer.
9. Attach the restored drive as near to the original configuration as possible (e.g., if the drive was originally on IDE channel 0 on the original computer, install it there.) This will help the computer to allocate the original drive letters, providing the proper mapping for .lnk files, etc.
10. On older drives less than 8.4 GB, you may need to reboot using an EnCase Barebones Boot Diskette, and during the boot sequence set the CHS settings of the restoration drive in the CMOS to the physical drive geometry of the original drive, which you noted earlier. Setting the physical drive geometry will probably require overriding the auto-detected drive geometry.
11. Use LinEn to calculate the hash value of the restored drive, and compare it to the acquisition hash value to ensure its integrity.
12. If you want to boot the drive, use an EnCase Barebones Boot Disk with FDISK copied to it. Run FDISK /MBR. The restored disk should now be bootable. Be aware that as soon as you boot it, the underlying data will be altered.

Note that differences may occur depending on whether you are restoring an NTFS or FAT32 file system, and whether the restored drive is being booted on the original hardware platform the drive was acquired from. EnCase applications restore using one of the following methods:

- Without FastBloc SE
- With FastBloc SE

Restoring without FastBloc SE, because the disk drivers for Windows 2000, XP and 2003 do not allow direct disk access, can be performed through the ASPI layer. ASPI has a problem with rounding off the last few sectors that do not fit on the last cylinder of a drive. This is the reason why all sectors are visible when the drive is read, yet when writes are attempted a small number of sectors may be missing. This is a Windows/ASPI limitation, not EnCase. Because of this limitation, you may need to use a slightly larger drive when performing the restore.

If you purchased the FastBloc SE module, you can restore to a drive that is controlled through FastBloc SE. When you restore with FastBloc SE, FastBloc SE replaces the Windows drivers and allows direct disk access, thereby circumventing the ASPI layer and its associated problems. Because FastBloc SE can write directly to the disk, you can restore to the same size drive.

Drive manufacturers also state that even though drives may appear identical, once partitioned they may not have the same capacity. If possible, drives from the same batch should be used so that both will be read with the same capacity (check the date on the drive's label). Older hard drives may have 2 platters, while the newer version may only have one, with the single platter drive having a few less bytes available.

## Logical Restore

Media have different types depending on the CHS (cylinders- heads-sectors) information. The same type might have different cylinders settings, but their heads and sectors information (the HS in CHS) will be the same. If the heads- sectors information is different, then the media type differs and you should use another target restore hard drive. A logical volume must be restored to a volume of the same size, or larger, and of the same type.

To prepare for a logical restore, the target media should be:

- wiped
- FDISKed
- partitioned
- formatted prior to restore

Format the target drive with the same file-type system as the volume to be restored (e.g., FAT32 to FAT32, NTFS to NTFS, etc.).

The procedure for restoring a logical volume is identical to that of restoring a physical device.

For a logical volume:

1. In Case view, right-click on the volume.
2. Select **Restore**.

When you finish the logical restore, a confirmation message displays. You must restart the computer to allow the restored volume to be recognized. Note that the restored volume contains only the information that was inside the selected partition.

## Booting the Restored Hard Drive

After the restore operation has finished with no errors, remove the target hard drive from the storage system and place it into a test system. Switch the power on. Depending on what operating system the subject ran, the test system should boot up exactly as the subject computer.

There are quite a few difficulties that can occur at this stage of the investigation. The most common is that the clone of the subject drive will not boot. Before trying anything else, check the restored disk using FDISK and verify it is set as an Active drive. If not, set the drive as Active (using the FDISK utility) and it should boot.



To boot the restored hard drive:

1. Ensure the intended restoration drive is at least as large as the original from which the image was taken.
2. Install a sterile restoration drive to your forensic machine, using a connection other than IDE 0. Note: EnCase cannot restore a physical drive to IDE 0.
3. Create but, do not format a single partition on the restoration drive.
4. Using Report pane, note the disk geometry of the forensic image of the drive you are restoring from, so the physical geometry used is correct.
5. Restore the forensic image of the physical drive to the restoration drive using the Restore Drive setting.
6. To make the restored drive active in Windows, right-click **My Computer** and select **Manage > Disk Management**, and then right-click the restored drive and select **Make Active**.
7. Shut down the computer and attach the restored drive as near to the original configuration as possible. This helps the computer to allocate the original drive letters, making .lnk files, etc. work better.
8. Reboot and set the CHS settings of the restoration drive in the CMOS to the physical geometry of the original drive, overriding the auto-detected geometry if necessary.

The restored disk should now be bootable.

## If the Restored Disk Does Not Boot

The Cylinders-Heads-Sectors information (CHS) in the Master Boot Record (MBR) from the image may not match the CHS information of the actual hard drive.

Reset the CHS information for the MBR. Boot with a DOS boot disk and, at the A:\> prompt, type `FDISK/MBR` to reset the Master Boot Record.

Verify that the MBR has the correct `io.sys` file. Re-SYS the boot drive with the correct `sys` version. For example, if the subject had Windows 95B, then the hard drive should have a `sys` command performed on it from a Windows 95B-created boot disk. At the A:\> prompt, type `SYS C:`

## Snapshot to DB Module Set

This script takes snapshots of nodes across a network and stores the snapshots in a SQL database. It also reads from the database to create reports on the snapshots taken. It allows for minimal maintenance on the database so you can control the amount of data stored as well.

Three EnScripts work with the database to perform their tasks:

- ☐ Initialize Database.EnScript
- ☐ Snapshot to DB.EnScript
- ☐ Snapshot DB Reports.EnScript

Each is discussed in detail below.

### Initializing the Database

The Initialize Database.EnScript:

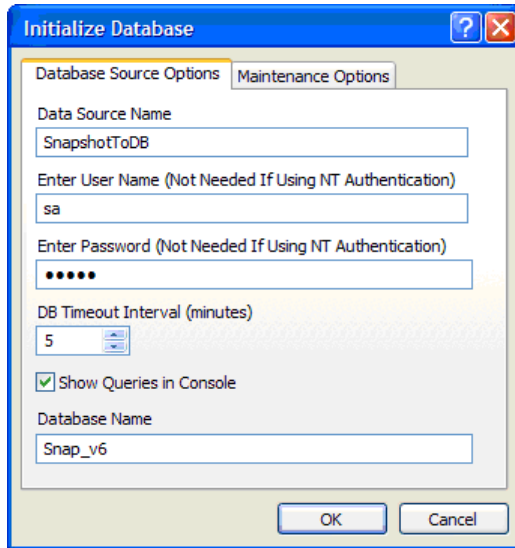
- ☐ initializes the database
- ☐ maintains the database

---

You must run this script first.

---

1. Make sure you set up an ODBC connection properly and note down the information used for that connection.
2. Run Initialize Database.EnScript. The Initialize Database dialog opens:



## Choosing Database Sources

Select the Database Source Options tab to specify connection information for the database:

**Data Source Name:** This is the name you gave the ODBC connection when you created it.

**Enter User Name (Not Needed If Using NT Authentication):** Specify a user name. If you set up the ODBC connection to use NT Authentication, it remembers your user name so you do not need to enter it manually.

**Enter Password (Not Needed If using NT Authentication):** Like your user name, you must specify a password to gain access to the database. If you set up the ODBC connection to use NT Authentication, it remembers your password so you do not need to enter it manually.

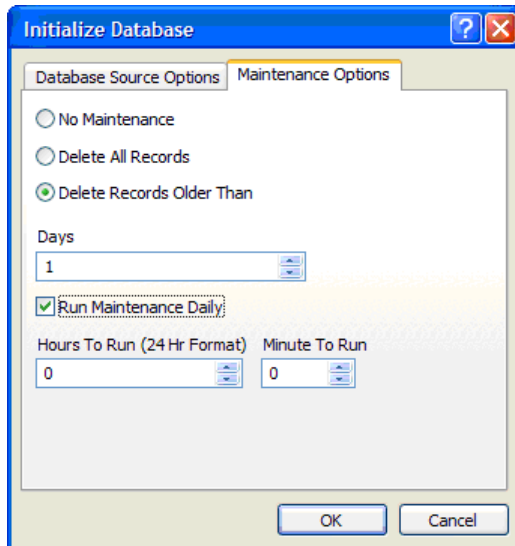
**DB Timeout Interval (minutes):** Specify how long you want to wait before a DB timeout occurs. This indicates how long the program waits before assuming the connection is bad (the default is 5 minutes).

**Show Queries in Console:** Check this box to produce comments on what is happening behind the scenes.

**Database Name:** Since a database management system can house many databases, you must specify the one you want to use.

## Maintaining the Database

1. Run Initialize Database.EnScript. The Initialize Database dialog opens:



2. Select the Maintenance Options tab to run basic cleaning maintenance on the database itself (including deleting database records) and fill in the various fields or check the appropriate box:

No Maintenance: Use this option if you want to initialize the database (selected by default).

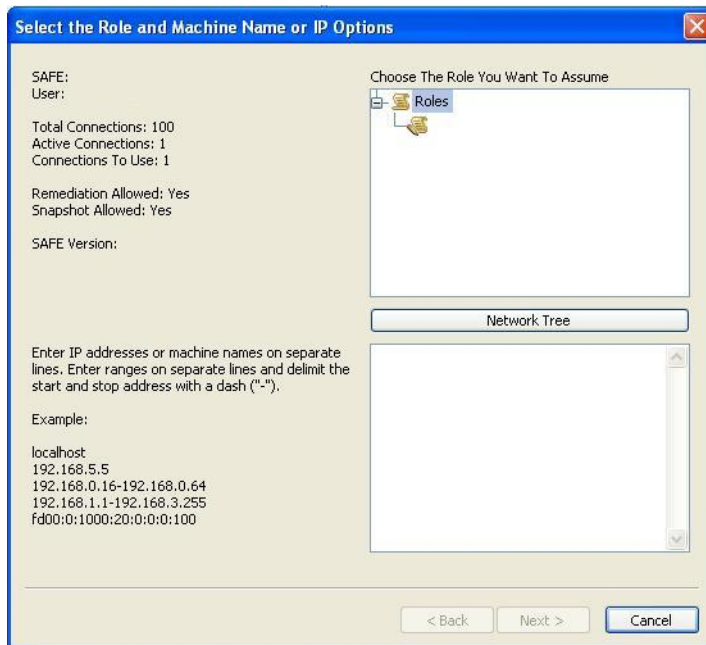
Delete All Records: Once a database is created, select this option to delete the entire contents in the database (but not the database itself).

Delete Records Older Than: You can automatically schedule cleaning the database by selecting this option. With this option selected, the following options become active and configurable:

- ☐ Days: Specifies the age of a record you want to delete. For example, selecting "1" means you want to delete records at least one day old.
- ☐ Run Maintenance Daily: This check box runs the cleaner every day at specified hours and minutes.

## Updating the Database

1. Run Snapshot To DB.EnScript. You will be required to log into a SAFE. When you successfully log in, this dialog opens:



This is where you:

- ☐ specify the nodes you want to scan
- ☐ take a snapshot

Choose the Role You Want to Assume: in the tree, select the specific role you want to use when connecting to the nodes.

---

Be sure to select a valid Role to enable the **Next** button.

---

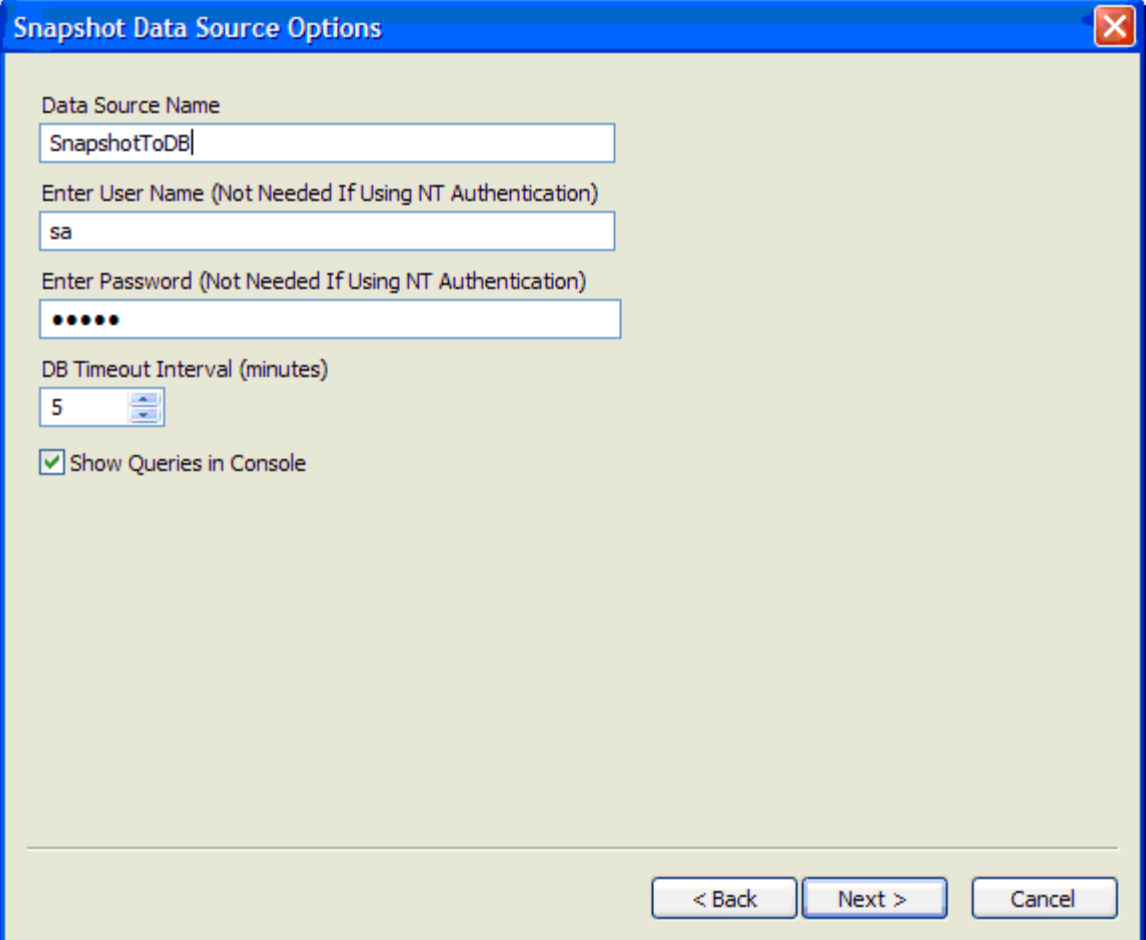
Click **Network Tree** to open a dialog where you can select nodes added to the role via SAFE.

Lower text box (under Network Tree): manually enter IP addresses, hostnames, and ranges here.

- ☐ Valid ranges must be defined as such: IPAddress1 "-" IPAddress2
- ☐ IPAddress2 must be greater than IPAddress1; that is, , IPAddress1 is the lowest IP Address in the range and IPAddress2 is the highest IP Address.

2. Once you specify which nodes to scan for snapshots, you must specify which database to use.

3. Click **Next**. The Snapshot Data Source Options dialog opens:



The screenshot shows a Windows-style dialog box titled "Snapshot Data Source Options". It contains several input fields and a checkbox. The "Data Source Name" field is filled with "SnapshotToDB". The "Enter User Name (Not Needed If Using NT Authentication)" field is filled with "sa". The "Enter Password (Not Needed If Using NT Authentication)" field is filled with seven dots. The "DB Timeout Interval (minutes)" is set to "5" in a spin box. The "Show Queries in Console" checkbox is checked. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

**Data Source Name:** This is the name you gave the ODBC connection when you created it.

**Enter User Name (Not Needed If Using NT Authentication):** Specify a user name. If you set up the ODBC connection to use NT Authentication, it remembers your user name so you do not need to enter it manually.

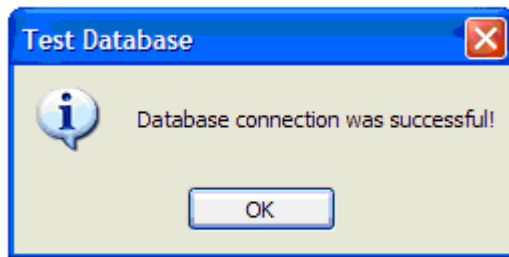
**Enter Password (Not Needed If using NT Authentication):** Like your user name, you must specify a password to gain access to the database. If you set up the ODBC connection to use NT Authentication, it remembers your password so you do not need to enter it manually.

**DB Timeout Interval (minutes):** Specify how long you want to wait before a DB timeout occurs. This indicates how long the program waits before assuming the connection is bad (the default is 5 minutes).

**Show Queries in Console:** Check this box to produce comments on what is happening behind the scenes.

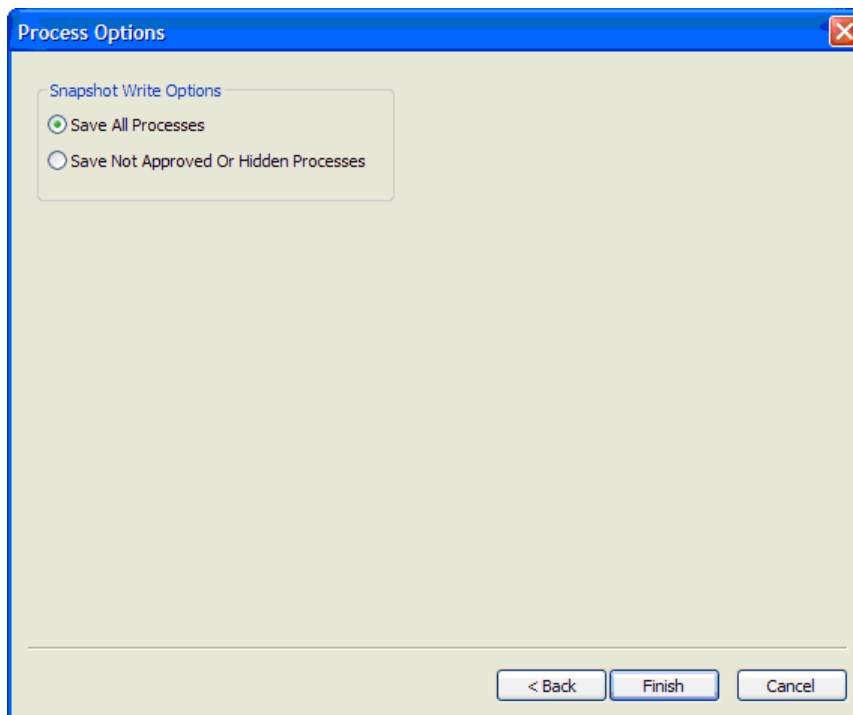
**Database Name:** Since a database management system can house many databases, you must specify the one you want to use.

4. Click **Next**. If the database connection is successful, a confirmation message displays:



## Specifying Database Content

Use the Process Options dialog to specify what information to insert into the database.



1. Select the appropriate Snapshot Write Options button:

Save All Processes takes a snapshot of each node and inserts these items into the database:

- ☐ Process
- ☐ Net users
- ☐ Net interfaces
- ☐ Open ports

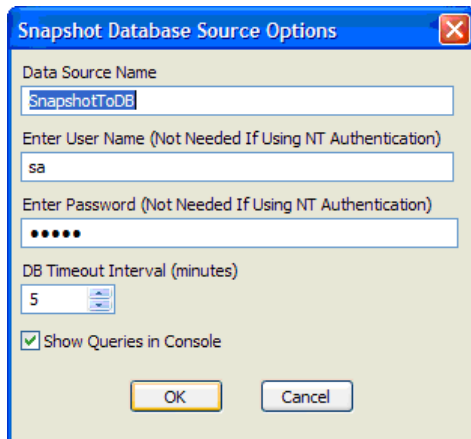
Save Not Approved Or Hidden Processes inserts not approved or hidden processes into the database.

2. Click **Finish** to begin the scanning process.

## Generating Reports on the Database

Once you gather data into the database, you can generate reports.

1. Run Snapshot DB Reports.EnScript. The Snapshot Database Source Options dialog opens:



Data Source Name: This is the name you gave the ODBC connection when you created it.

Enter User Name (Not Needed If Using NT Authentication): Specify a user name. If you set up the ODBC connection to use NT Authentication, it remembers your user name so you do not need to enter it manually.

Enter Password (Not Needed If using NT Authentication): Like your user name, you must specify a password to gain access to the database. If you set up the ODBC connection to use NT Authentication, it remembers your password so you do not need to enter it manually.

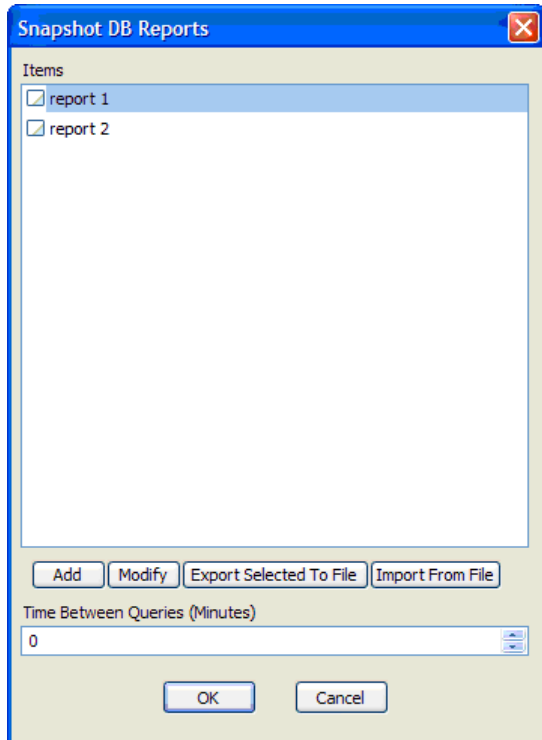
DB Timeout Interval (minutes): Specify how long you want to wait before a DB timeout occurs. This indicates how long the program waits before assuming the connection is bad (the default is 5 minutes).



Show Queries in Console: Check this box to produce comments on what is happening behind the scenes.

Database Name: Since a database management system can house many databases, you must specify the one you want to use.

2. Click **OK**. The Snapshot DB Reports dialog opens:



3. Select the check box for the reports you want to generate.
4. Click **OK** to begin generating the report.

## Using the Snapshot DB Reports Dialog

This dialog lists reports generated from the database snapshot. You can add or modify reports, as well as export reports to a file or import them from a file.

### Items

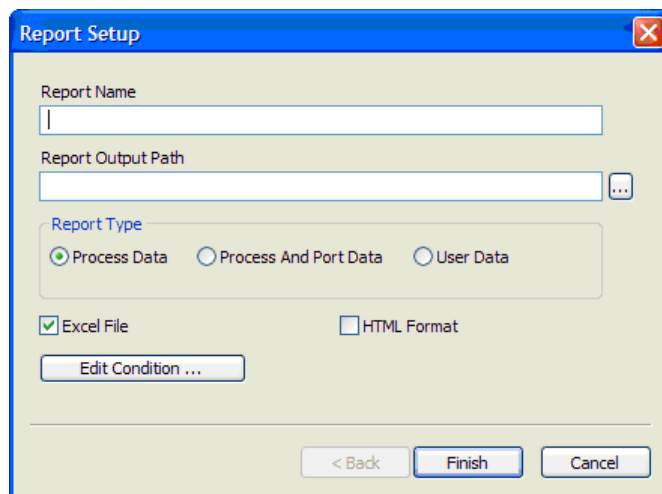
This list box contains information on reports already generated. If you create or add a report, that report and the options you select for it are stored in the database, enabling you to regenerate it as needed.

Double-click an item in the list to modify it.

Right-click an item to delete it. If you delete an item without selecting its check box, you must click **OK** and then click **Yes** on the resulting warning message.

### Add

Click **Add** to create a new report definition. The Report Setup dialog opens:



In the Report Name field, specify the name of the report.

In the Report Output Path field, specify the location to save the report.

In Report Type, select the type of report you want to generate:

- ☐ Process Data
- ☐ Process and Port Data
- ☐ User Data

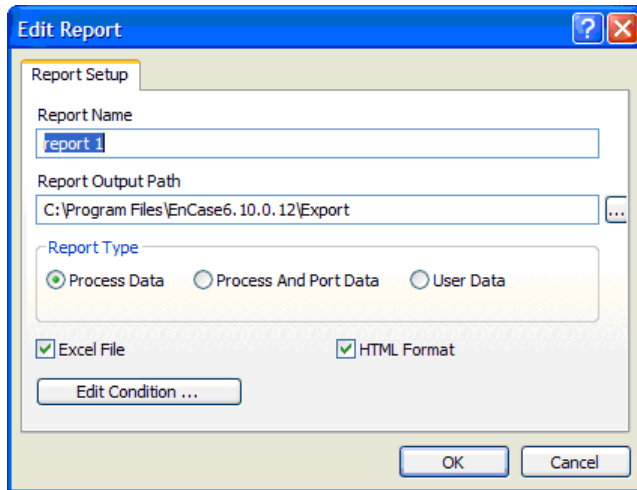
Excel File: Select to output the report as a Microsoft Excel file.

HTML Format: Select to output the report as an HTML file.

Edit Condition....: Select to add a set of conditions to report on.

## Modify

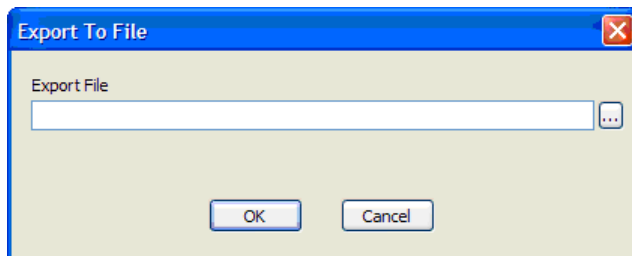
Select an item in the list, making sure the check box is cleared, then click **Modify**. The Edit Report dialog opens:




Make the modifications you want, then click OK. The modifications are saved to the database.

## Export Selected to File

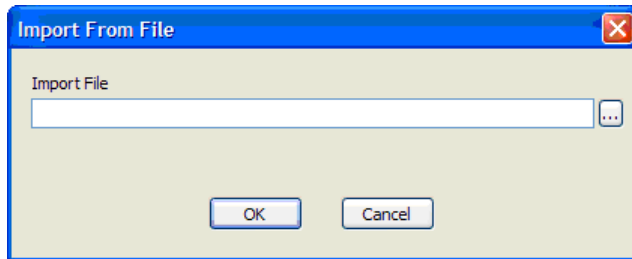
Click **Export Selected To File** to export a report definition from the database. The Export To File dialog opens:



Click the **Browse** button  to specify where to save the report definition, then click **OK**.

### Import from File

Click **Import from File** to import a report definition to the database. The Import from File dialog opens:



Click the **Browse** button  to locate the file to import, then click **OK**.

### Time between Queries (Minutes)

Enter or select the number of minutes you want to pause between queries.



## WinEn

WinEn is a standalone command line utility that captures the physical memory on a live computer running a Windows operating system (Win2k or higher). The physical memory image captured by WinEn is placed in a standard evidence file, along with the user-supplied options and information.

WinEn runs from a command prompt on the computer where you want to capture the memory. WinEn has a very small footprint in memory, and it is typically run from a removable device such as a thumb drive. Although this method makes minor changes to the computer running WinEn, this is the most effective way to capture physical memory before shutting down a computer. As always, it is recommended that examiners document and explain their procedures for later reference.

## Running WinEn

To run WinEn, open a command prompt on the target computer. The user logged on must have local administrator privileges on the computer, and you must start the command prompt with that privilege level. Once you open a command prompt, run WinEn using the syntax below. It is recommended that you compress the evidence file that is created and save it to removable media so that no additional changes are made to the target computer.

There are three ways to supply necessary information to WinEn when running from the command line:

- Command line options
- Configuration file
- Prompt for value

## Command Line Options

Syntax: **winen** <option> <option>

-p <EvidencePath>*	Path and file name of the evidence file to be created (maximum 32768 characters)
-d <Compress>*	Level of compression (0=none, 1=fast, 2=best)
-e <Examiner>*	Examiner's name (maximum 64 characters)
-m <EvidenceName>*	Name of the evidence within the evidence file (maximum 50 characters)
-c <CaseNumber>*	Case number related to the evidence (maximum 64 characters)
-r <EvidenceNumber>*	Evidence number (maximum 64 characters)
-s <MaxFileSize>	Maximum file size of each evidence file segment in MB (default: 640, minimum: 1, maximum: 10737418240)
-g <Granularity>	Error granularity in sectors (default: 1, minimum: 1, maximum: 1024)
-b <BlockSize>	Sectors per block for the evidence file (default: 64, minimum: 1, maximum: 1024)
-t	Compute HASH while acquiring the evidence (default: TRUE, values: TRUE or FALSE)
-a <AlternatePath>	A semicolon-delimited list of alternate paths (maximum 32768 characters)
-n <Notes>	Notes (maximum 32768 characters)
-f <Configuration File>	Path to a configuration file holding variables for the program (maximum 32768 characters)
-h	Help message

\* = Required field

## Configuration File

You can create a configuration file to fill in some or all of the variables. The configuration file needs to be in the format `OptionName=Value`, and can be used in conjunction with command line options.

All of these options have the same restrictions as their command line counterparts.

---

Note that options entered on the command line will override the same option in the configuration file. This way, users can override a specific setting in the configuration file by entering the appropriate information on the command line.

---

**Options for the configuration file are as follows:**

EvidencePath*	Path and file name of the evidence file to be created (maximum 32768 characters)
Compress*	Level of compression (0=none, 1=fast, 2=best)
Examiner*	Examiner's name (maximum 64 characters)
EvidenceName*	Name of the evidence within the evidence file (maximum 50 characters)
CaseNumber*	Case number related to the evidence (maximum 64 characters)
EvidenceNumber*	Evidence number (maximum 64 characters)
MaxFileSize	Maximum file size of each evidence file segment in MB (minimum: 1, maximum: 10737418240)
Granularity	Error granularity in sectors (minimum: 1, maximum: 1024)
BlockSize	Sectors per block for the evidence file (minimum: 1, maximum: 1024)
Hash	Compute HASH while acquiring the evidence (TRUE or FALSE)
AlternatePath	A semicolon-delimited list of alternate paths (maximum: 32768 characters)
Notes	Notes (maximum: 32768 characters)

\* = Required field

## Configuration File Notes

- You can use the pound sign (#) as a comment delimiter. Anything after a pound sign on a line is ignored.
- Empty lines in the configuration file are ignored.
- Options in the configuration file are not case-sensitive.
- White space before or after the <option> and before or after the <value> is ignored. White space in the middle of an option is retained (such as a space between an examiner's first and last name).

## Prompt for Value

The console asks for any required (\*) values (Please enter a value for the option <option>) if they are not provided in one of the formats above.

## Error Handling

The program checks all values entered to make sure they conform to expectations. Any deviation causes the program to exit or prompt for a correct value.

## Additional WinEn Information

- **Progress Bar:** While the process is running it uses hash (|) marks across the screen as a status indicator, using the full width of the screen as the 100% mark.
- **Cancel:** To stop the process while it is running, use the CTRL-BREAK (or CTRL-C) key combination.
- **WinEn Driver:** At run time, WinEn drops its driver file in the same directory where WinEn is running. This driver is named **WinEn.sys** or **WinEn64.sys**.
- **Changes to target system:** When WinEn runs on a system, the following changes can be expected:
  - ☐ When executed, WinEn loads into memory on the target system. This is unavoidable and will take up approximately 2.8 MB of RAM.
  - ☐ Windows Service Control Manager creates registry keys when it loads the WinEn driver. These keys are typically stored in:
    - HKEY\_LOCAL\_MACHINE\SYSTEM\<ControlSet>\Enum\Root\LEGACY\_WINEN\_
    - HKEY\_LOCAL\_MACHINE\SYSTEM\<ControlSet>\Services\winen\_
  - ☐ Data is written to the PageFile based on operating system memory use.



- **Renaming WinEn:** As noted above, WinEn leaves remnants on the system where it is run. If desired, you can rename the WinEn executable so that the remnants are obfuscated. Renaming the executable also causes the WinEn driver to be renamed similarly.



# Viewing File Content

- Viewing Files 278
- File Viewers 292
- View Pane 296
- Viewing Compound Files 297
- Viewing Base64 and UUE Encoded Files 316
- NTFS Compressed Files 318
- Gallery Tab 318
- Lotus Notes Local Encryption Support 321

## Viewing Files

Files parsed from device previews and acquisitions can be viewed in various formats. EnCase Enterprise supports viewing the following files:

- Text (ASCII and Unicode)
- Hexadecimal
- Doc, native formats for Oracle Outside In technology supported formats
- Transcript, extracted content with formatting and noise suppressed
- Various image file formats

The Doc pane and the Transcript pane use Oracle Outside In technology to display hundreds of different documents.

This allows investigators to view documents without owning a copy of the application in order to view the contents. It also allows the investigator to bookmark an image of the contents inside a particular application (such as a database), or it allows bookmarking exact text inside the document using a sweeping bookmark.

Beyond those formats supported by the EnCase applications, investigators can use third-party viewers to extend the range of files they can view. Once the investigator adds the viewer to their environment and associates file extensions with the viewer, the files of that type can be viewed.

Compound files contain other files. Examples of compound files include email messages and their attachments or zip files and the files they contain. Viewing compound files expose their file structure.

EnCase Enterprise can view the structure of these types of compound files:

- Outlook Express (DBX)
- Outlook (PST)
- Exchange 2000/2003 (EDB)
- Lotus Notes (NSF) for versions 4, 5, and 6
- Mac DMG Format
- Mac PAX Format
- JungUm Korean Office documents
- Zip files such as ZIP, GZIP, and TAR files
- Thumbs.db files
- Others not specified

Some audio files, video files and certain graphic file formats are not immediately viewable; however, investigators can associate third-party viewers to examine these files properly.

## Copying and Unerasing Files and Folders

EnCase® Software recovers and unerases files on a byte-per-byte basis. This feature is called Copy/UnErase. Use the unerase function to view deleted files within Windows.

Deleted files on a FAT volume have a hex \xE5 character at the beginning. EnCase applications allow you to replace this character with one of your choice. The underscore ( \_ ) character is used by default. The Copy/UnErase wizard provides settings for unerasing the file and the character used to replace the deleted file character.

## Copy and Unerase Features

EnCase applications provide the following Copy and Unerase Features:

- Copy/Unerase Wizard
- Copy Folders Dialog

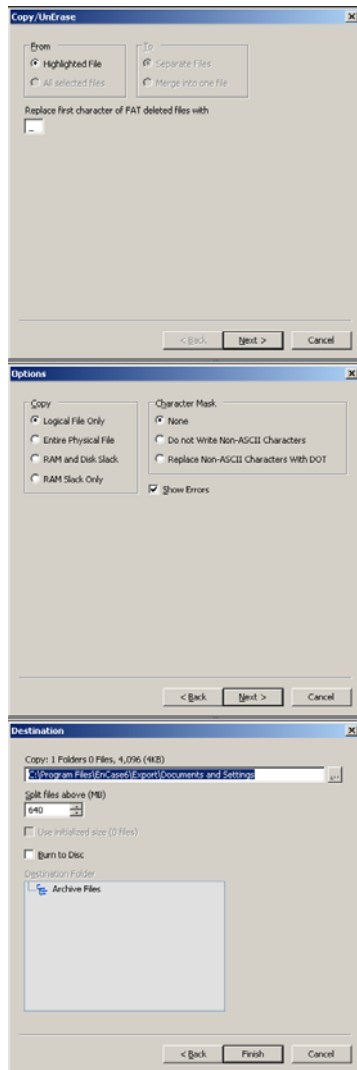
---

Note: The Copy/Unerase functionality does not preserve folder structure, while Copy Folders functionality does.

---

## Copy/UnErase Wizard

Use the Copy/UnErase wizard to specify what files are unerased, how they are unerased, and where the files are saved after they are unerased.

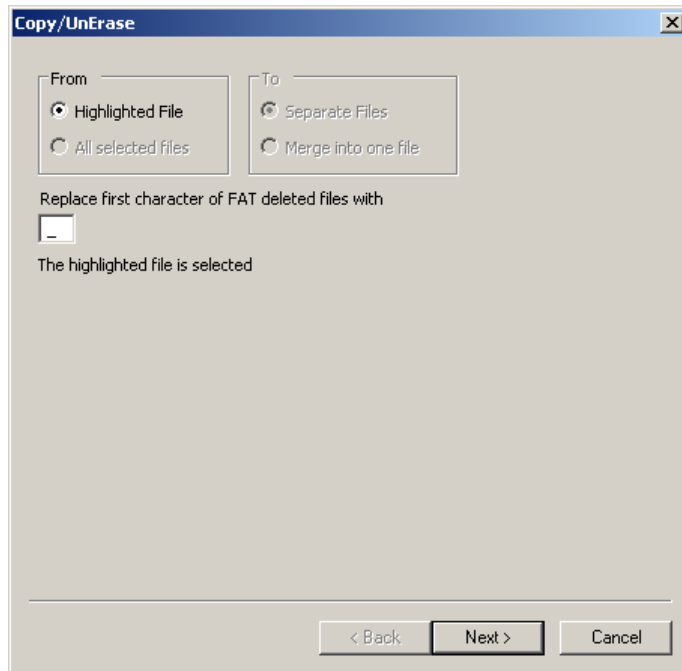


The Copy/UnErase wizard consists of

- File Selection page
- Options page
- Destination page

## File Selection Page of the Copy/UnErase Wizard

The File Selection page of the Copy/UnErase wizard indicates whether a single file or a set of selected files are being copied and unerase. In addition, the character that will be used to replace the character that FAT volumes use to indicate deleted files is set here.



**From** contains the settings that determine if one file or several files will be copied and unerased.

**Highlighted File:** If no files are selected in the Table pane, choose this setting because at least one file is always highlighted on the Table pane. The highlighted file will be copied and unerased.

**All selected files:** When several files are selected in the Table pane, use this setting. When you choose this setting, you have the option to copy and unerase the highlighted file, or the selected files.

**To** contains settings to determine how many files will be output, which is only relevant when several files were selected to be copied and unerased.

**Separate Files** outputs each file being copied and unerased to its own file.

**Merge into one file** merges the output of all the selected files into one file.

**Replace first character of FAT deleted files with** determines which character is used to replace the first character in the filename of deleted files in the FAT file system.

**Status:** This line indicates if one file or several files will be copied and unerased.

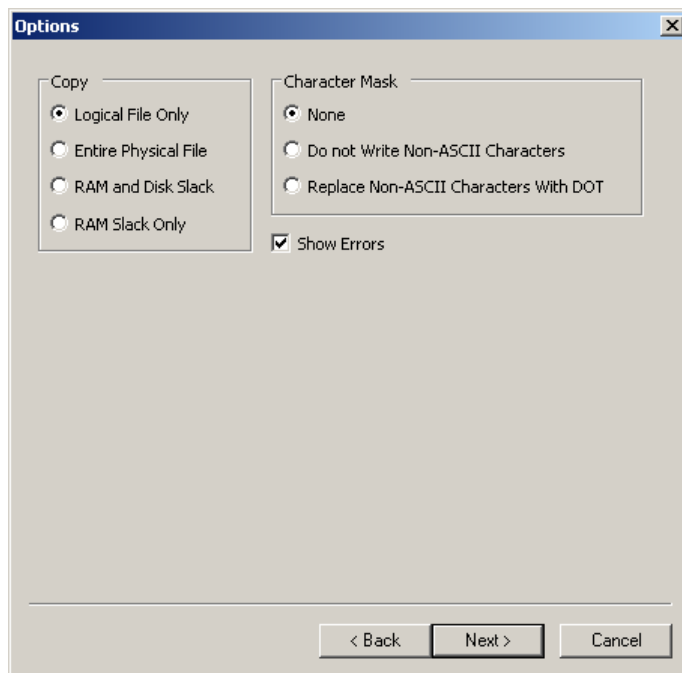


## Options Page of the Copy/UnErase Wizard

The Options page of the Copy/UnErase wizard determines:

- The extent of the evidence file copied
- Whether non-ASCII characters encountered will appear in the outputted file or files
- Whether dots will replace non-ASCII characters in the outputted file or files
- Whether errors in the files will pause the operation and wait for user input

Settings on this page involve RAM slack, which is the buffer between the logical area and the start of the file slack. RAM slack is sometimes referred to as sector slack.



**Copy** contains the settings that determine the extent of the content of the evidence file to be copied.

**Logical File Only:** Copy/Unerase is performed on the logical file only, which does not include the file slack.

**Entire Physical File:** Copy/Unerase is performed on the entire physical file, which includes the logical file and file slack.

**RAM and Disk Slack:** Copy/Unerase is performed on both the RAM and disk slack.

**RAM Slack Only:** Copy/Unerase is performed on the RAM slack only.

**Character Mask** contains settings that determine what characters are written into the file or files created by the Copy/UnErase operation.

**None:** No characters are masked or omitted from the filenames of the resulting files.

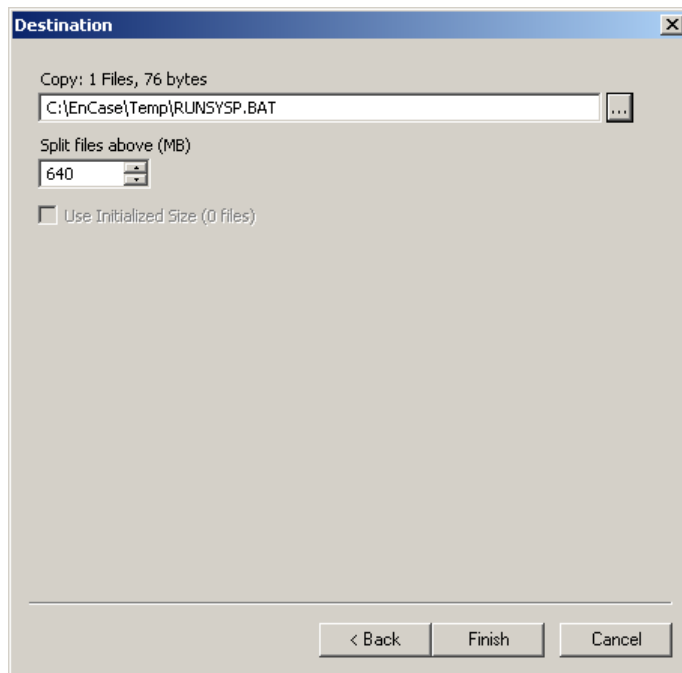
**Do not Write Non-ASCII Characters:** Non-ASCII characters are masked, or omitted, from the filenames of the resulting files. All characters except non-ASCII characters are used.

**Replace NON-ASCII Characters with DOT:** Non-ASCII characters are replaced with periods in the filenames of the resulting files.

**Show Errors:** The application queries the user when errors occur. This prevents unattended execution of the copy and unerase operation.

## Destination Page of the Copy/UnErase Wizard

The Destination page of the Copy/UnErase wizard determines where the output of the copy and unerase operation is saved, how many files will be created when a file to be output grows too large, whether the initialized size is used, and the destination folder containing the output of the copy and unerase operation.



**Copy** displays the number of files to be copied and unerased, and the total number of bytes that comprise the file or files being created.

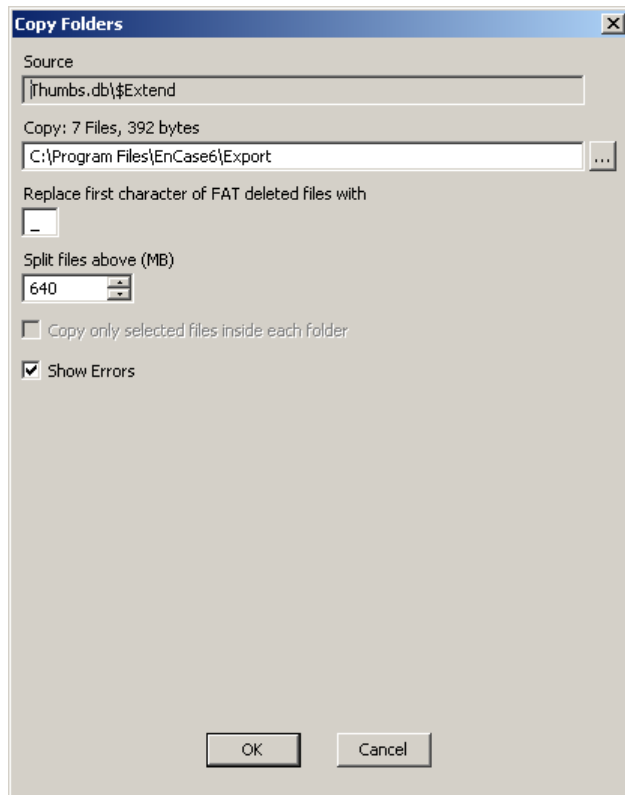
**Path** contains the path and filename, within the file system of the investigator's machine, of the file or files created.

**Split files above** contains the maximum length, not exceeding 2000MB, of any file created by the Copy/Unerase operation. When the total number of bytes comprising an output file exceeds this value, the additional output is continued in a new file.

**Use Initialized Size** determines if only the initialized size of an entry will be searched, as opposed to the logical size (which is the default) or the physical size. This setting is only enabled for NTFS file systems. When an NTFS file is written, the initialized size can be smaller than the logical size, in which case the space after the initialized size is zeroed out.

## Copy Folders Dialog

Use this dialog when copying entire folders selected in the Tree pane while preserving the folder structure.



**Source** displays the Entities folder being copied and unerasd.

**Copy** displays the number of files to be copied and unerasd, and the total number of bytes that comprise the file or files being created.

**Path** contains the path and filename, within the file system of the investigator's machine, of the file or files created.

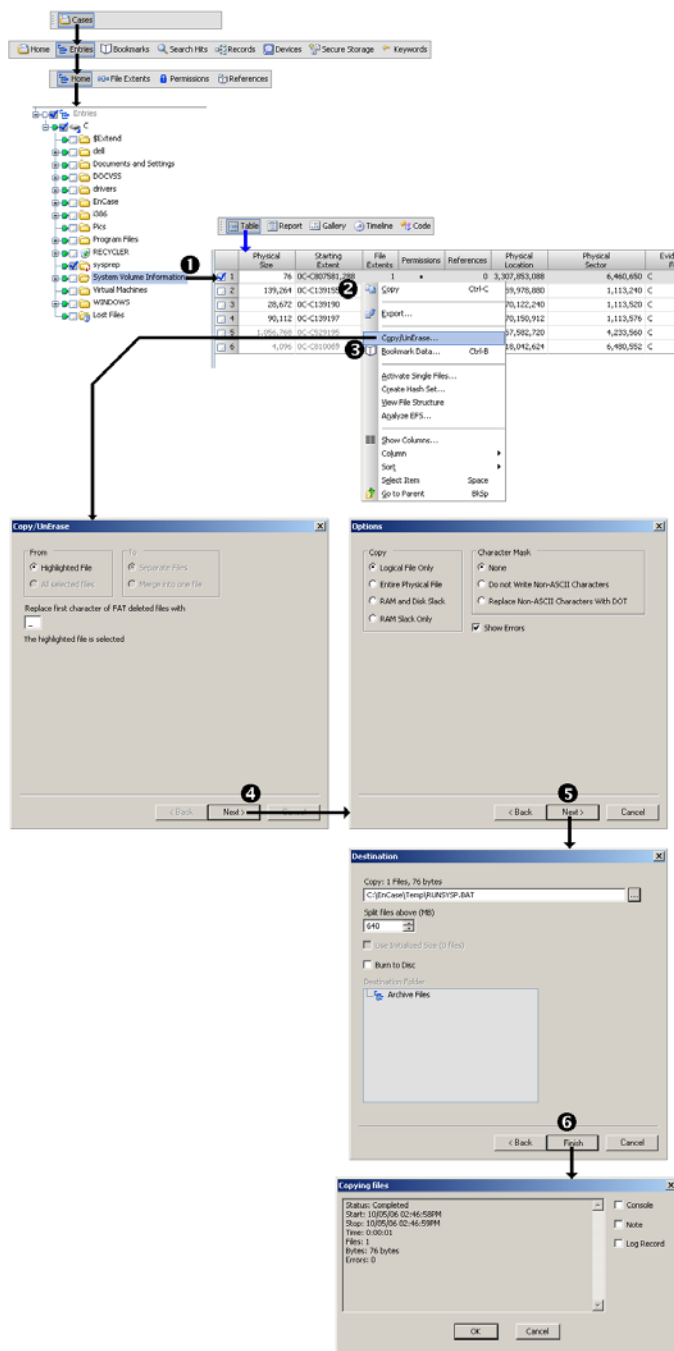
**Replace first character of FAT deleted files with** determines which character is used to replace the first character in the filename of deleted files in the FAT file system.

**Split files above** contains the maximum length, not exceeding 2000 MB, of any file created by the copy and unerase operation. When the total number of bytes comprising an output file exceeds this value, the additional output is directed to and continued in a new file.

**Copy only selected files inside each folder:** If individual files were selected within a folder or folders, this setting determines if only the files or all the files in the folder will be copied and unerasd.

**Show Errors:** When selected, the application does not query the user when errors occur. This allows unattended execution of the copy and unerase operation.

## Copying and Unerasing Files



### To copy and unerase a file

1. In the Tree pane, highlight the folder containing the file or files to be unerased.  
The Table pane displays the contents of the folder.
2. In the Table pane, highlight the file or select the files you want to unerase.

3. Right-click on the highlighted file and click **Copy/UnErase**.

The File Selection page of the Copy and UnErase wizard appears.

4. Complete the File Selection page of the Copy/UnErase wizard. For detailed instructions, see *Completing the File Selection Page*.
5. Click **Next**.

The Options page of the Copy/UnErase wizard appears.

6. Complete the Options page of the Copy/UnErase wizard. For detailed instructions, see *Completing the Options Page*.
7. Click **Next**.

The Destination page of the Copy/UnErase wizard appears.

8. Complete the Destination page of the Copy/UnErase wizard. For detailed instructions, see *Completing the Destination Page*.
9. Click **Finish**.

The copy and unerase operation executes. The resulting files are saved in the directory specified on the Destination page.

## Completing the File Selection Page

The File Selection page is the first page of the Copy/UnErase wizard.

1. If several files were selected on the Table pane before you opened the wizard:
  - a. Determine if the highlighted file, or the selected files should be copied and unerased.
  - b. Click either **Highlighted File**, or **All selected files**, as appropriate.
2. If several files were selected on the Table pane before you opened the wizard:
  - a. Determine if you want a collection of files or a single file as the result of the copy and unerase operation
  - b. Click either **Separate Files**, or **Merge into one file**, as appropriate.
3. If you want to use a character other than the underline character as the replacement for the FAT file system deleted file indicator, type the character into the **Replace first character of FAT deleted files with** field.
4. Click **Next**.

The Options page of the Copy/UnErase wizard appears.

## Completing the Options Page

The Options page is the second page of the Copy/UnErase wizard.

1. Determine the scope of what is to be copied and unerased, and click on the control that captures the appropriate scope.
2. Determine the type of mask you want to employ during the copy and unerase operation, and click on the control that uses the mask.
3. Decide if you want the copy and unerase operation to stop when it encounters an error, or continue execution even if errors are found. This is the same as asking if you want the copy and unerase operation to run unattended. For unattended execution, select **Show Errors**; otherwise, clear **Show Errors**.
4. Click **Next**.

The Destination page of the Copy/UnErase wizard appears.

## Completing the Destination Page

The Destination page is the last page of the Copy/UnErase wizard.

1. If desired, provide a path to and filename where the results of the Copy/Unerase operation will be saved.
2. If desired, change the **Split files above** value.
3. If **Use Initialized Size** is enabled and you want to use it, select **Use Initialized Size**.
4. Click **Finish**.

The copy and unerase operation begins. As it runs, the thread status line provides an indication of progress. When the thread completes, a results dialog is displayed. The results are saved in the appropriate folder in the file system and, if requested, the results files are burned onto the disc in the default or specified directory.

---

Note: The thread status line provides an indication of progress.

---

## Copying and Unerasing Bookmarks

You can Copy/Unerase bookmarked files as well. The process is the same whether copying single or multiple bookmarks. If the file was deleted and resides in unallocated space, the Copy/UnErase wizard tries to copy the entire unallocated space, since the data pertaining to the file resides there.

1. On the Bookmark Tree tab, select the desired bookmark folder.
2. In the Table pane, select the desired bookmarks.



3. Right-click in the Table pane, and select **Tag Selected Files**.

The files associated with the deleted bookmarks are selected and consolidated on the Entries Table pane.

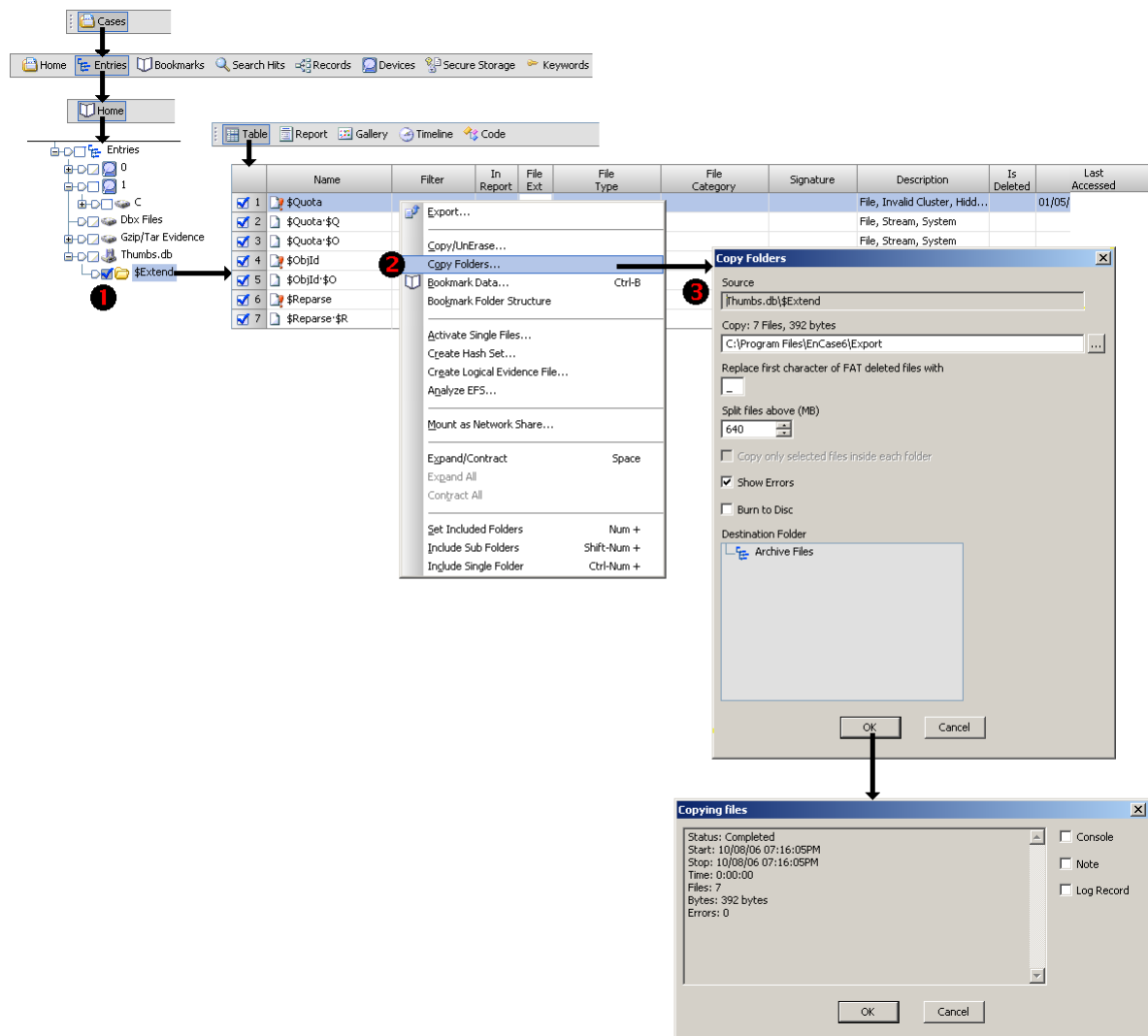
4. Move to the Entries pane, and in the Table pane, right-click one of the selected files.
5. Click **Copy/Unerase**.

The File Selection Page of the Copy/UnErase wizard appears.

6. Continue the copy and unerase process at step 4 of Copying and Unerasing Files

The files associated with the selected bookmarks are copied and unerased.

## Copying Folders



1. In the Tree pane, select the folder or folders to copy and unerase.
2. If desired, in the Table pane clear any individual files that should not be copied and uneraser.
3. Right-click in the Table pane, then select **Copy Folders**.

The Copy Folder dialog appears.

4. Modify the settings on this dialog as desired. For more information, see *Copy Folders Dialog* (on page 286).

The copy operation begins. As it runs, the thread status line provides an indication of progress. When the thread completes, a results dialog appears. The results are saved in the appropriate folder in the file system.

---

Note: The thread status line provides an indication of progress. You can terminate processing at the thread status line.

---

## File Viewers

Occasionally, an investigator finds file types that EnCase applications do not have the built-in capabilities to view, or you might want to view a file type using a third party tool or program. In either situation, you must:

- Add a file viewer to your EnCase application. See *Adding a File Viewer to your EnCase Application* (on page 294).
- Associate the file viewer's file types with the viewer. See *Associating the File Viewer's File Types with the Viewer* (on page 295).

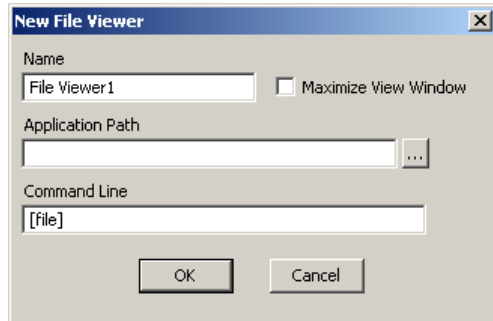
## File Viewer Features

EnCase applications provide the following file viewer features:

- New File Viewers Dialog
- View File Type Dialog

## New File Viewer Dialog

Use the New File Viewer dialog to add file viewers to your EnCase application.



**Name** is the name of the file viewer.

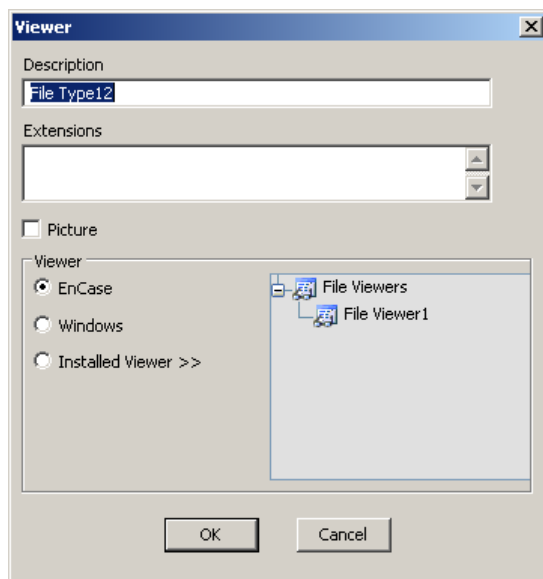
**Maximize View Dialog** check to open the file viewer in a maximized new window.

**Application Path** contains the filename and path to the viewer's executable.

**Command Line** contains a reference to the executable and any parameters used to customize the execution of the viewer.

## Viewer File Type Dialog

The Viewer File Type dialog associates file types with viewers.



**Description** is the file type to be associated with the file viewer.

**Extensions** is a list of file types to be associated with the file viewer.

**Picture:** check to display the file as a picture in the Gallery tab.

**Viewer** contains options selecting the type of viewer, and in the case of Installed Viewers, a specific viewer associated with the file type you define.

Click **EnCase** to associate the built-in EnCase viewer with the file type you define.

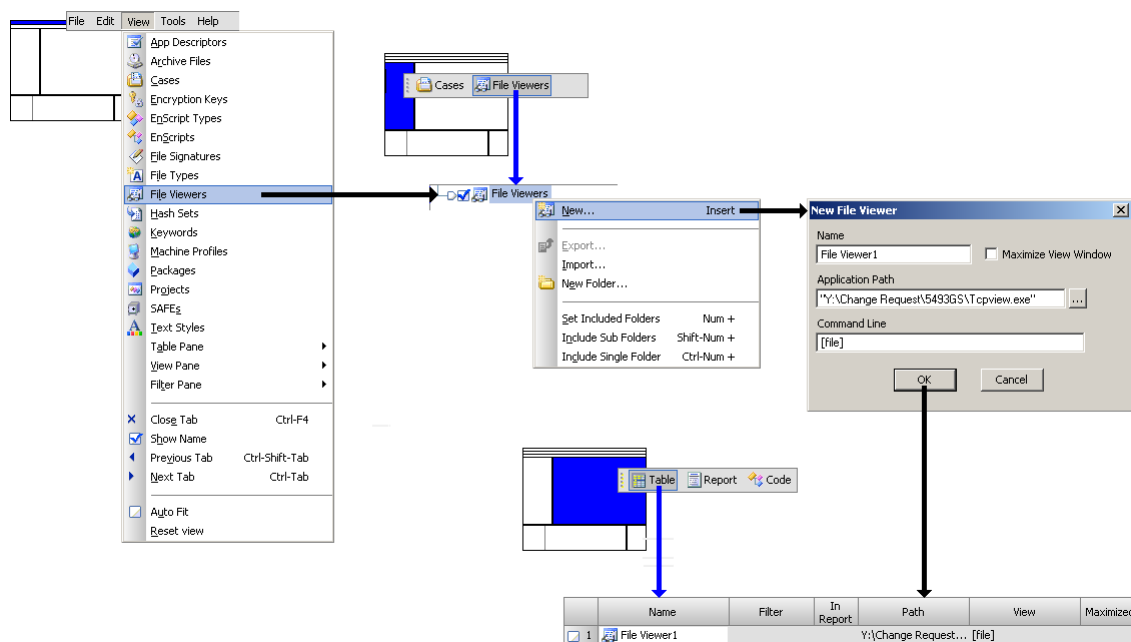
Click **Windows** to associate Windows with the file type you define.

Click **Installed Viewer** to associate an installed viewer with a file type. Use the Installed Viewers Tree to select the specific viewer.

**Installed Viewers Tree** lists the File Viewers currently known to your EnCase application.

## Adding a File Viewer to Your EnCase Application

Figure 30



1. Display the File Viewers tree in the Tree pane:
  - ☐ On the main window, click **View > File Viewers**, or
  - ☐ On the Tree pane, click **File Viewers**.

The File Viewer tree appears.

2. Right-click the root of the File Viewers tree, and select **New**.

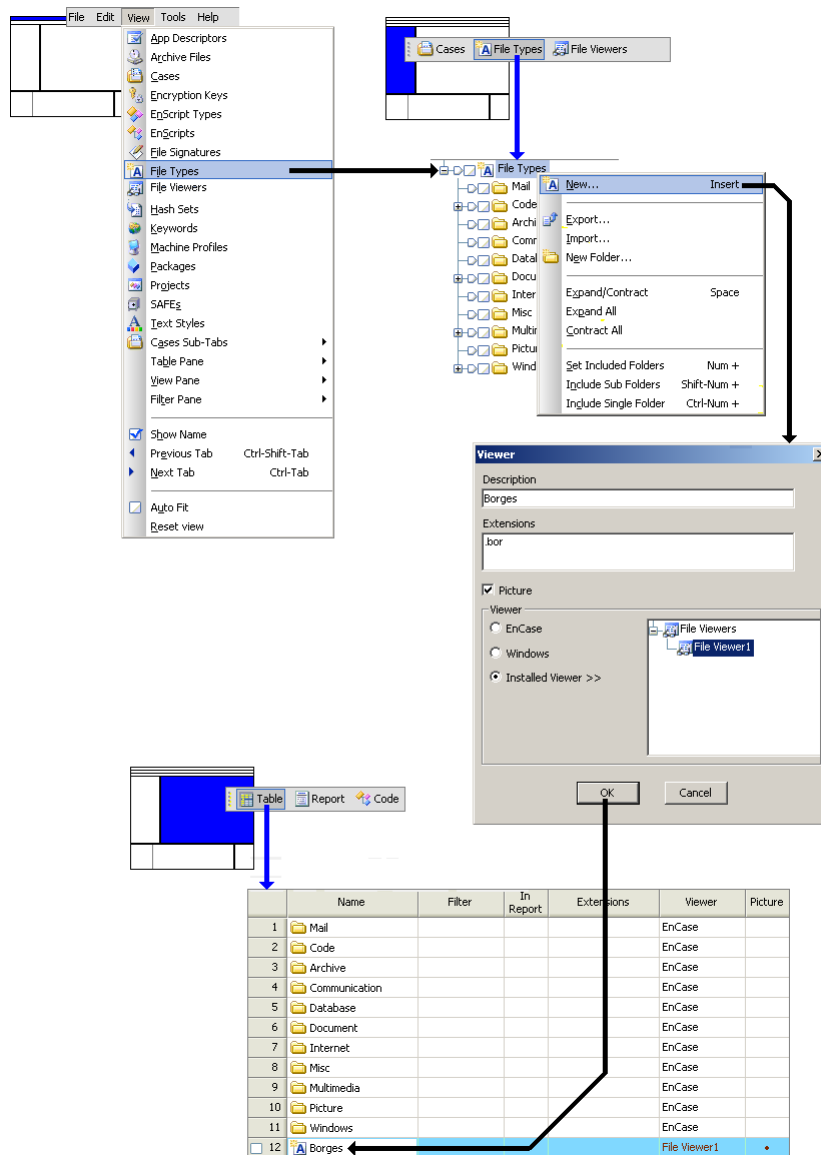
The New File Viewer dialog appears.

3. Browse to the file viewer's executable, make any other changes to the settings on the dialog, and click **OK**.

The file viewer appears in the file viewer table.

## Associating the File Viewer's File Types with the Viewer

When you add a new file viewer to your EnCase application, you must associate that viewer's file types.



1. Display the File Viewers tree in the Tree pane:

- ☐ On the main window, click **View > File Types**, or
- ☐ On the Tree pane, click **File Types**.

The File Types tree appears.

2. Right-click on the root of the File Types tree, and select **New**.

The Viewer File Type dialog appears.

3. In the **Viewer** box, click **Installed Viewer** and select the file viewer to associate with the file type from the File Viewers tree.
4. Enter a description and the file extensions of the file types.
5. If the file viewer displays pictures, check **Picture**.
6. Click **OK**.

The files entered are now associated with the selected file viewer.

## View Pane

The View pane provides several ways to view file content:

- The **Text** tab allows you to view files in ASCII or Unicode text
- The **Hex** tab allows you to view files as straight Hexadecimal.
- The **Doc** tab provides native views of formats supported by Oracle Outside In technology.
- The **Transcript** tab displays the same formats as the Doc tab, but filters out formatting and noise, allowing you to view files that cannot display effectively in the Text tab.
- The **Picture** tab allows you to view graphic files.

## Viewing Compound Files

You can view the individual components of compound files within an evidence file.

Compound files are typically comprised of multiple layers containing other files. You can view these times of compound files in the EnCase application:

- Registry Files
- OLE Files
- Compressed Files
- Lotus Notes
- MS Exchange
- Outlook Express email
- MS Outlook email
- Windows Thumbs.db
- American Online ART Files
- Hangul Korean Office documents
- Macintosh PAX files

---

Note: In addition, the File Mounter EnScript® program allows the examiner to select a file type (DBX, GZip, PST, Tar, Thumbs.db or Zip), provided they have a valid signature, and mount them automatically.

---

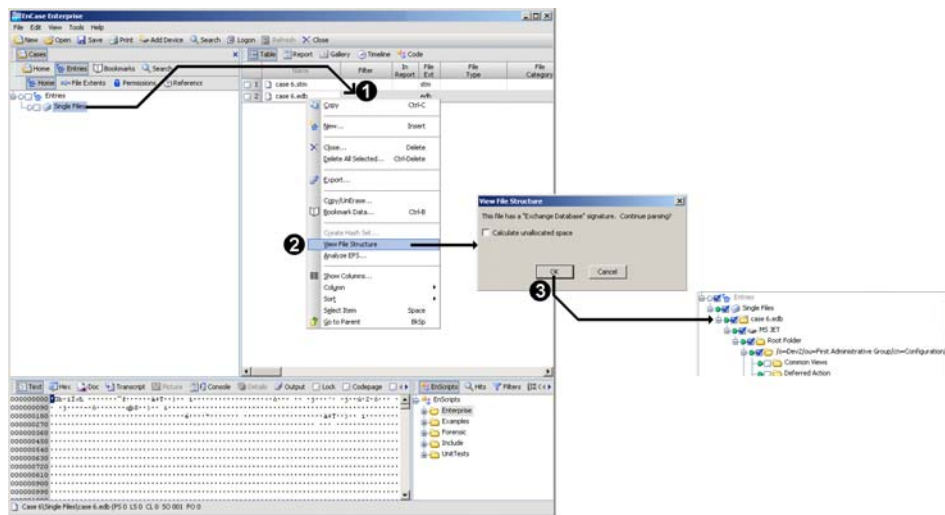
## Viewing File Structure

Once files are part of the case, they can be viewed in various output formats. Viewing the structure of a compound file reveals which files comprise it.

Before you begin:

1. Open a case.
2. Enable single files.
3. The Entries tree on the Entries tab and Entries table are displayed.

4. Drag and drop the files to be viewed into the Entities table in the Table pane.



*To view a compound file:*

1. Navigate to the compound file to be viewed as it appears in the Table pane.
2. Right-click the compound file to be viewed, and click **View File Structure**.

The View File Structure message box appears.

3. Click **Yes**.

The compound file is replaced in the Tree pane and Table pane with a folder and a compound volume icon.

The file structure of the compound file displays, and component files display in the view of your choice.



## Viewing Registry Files

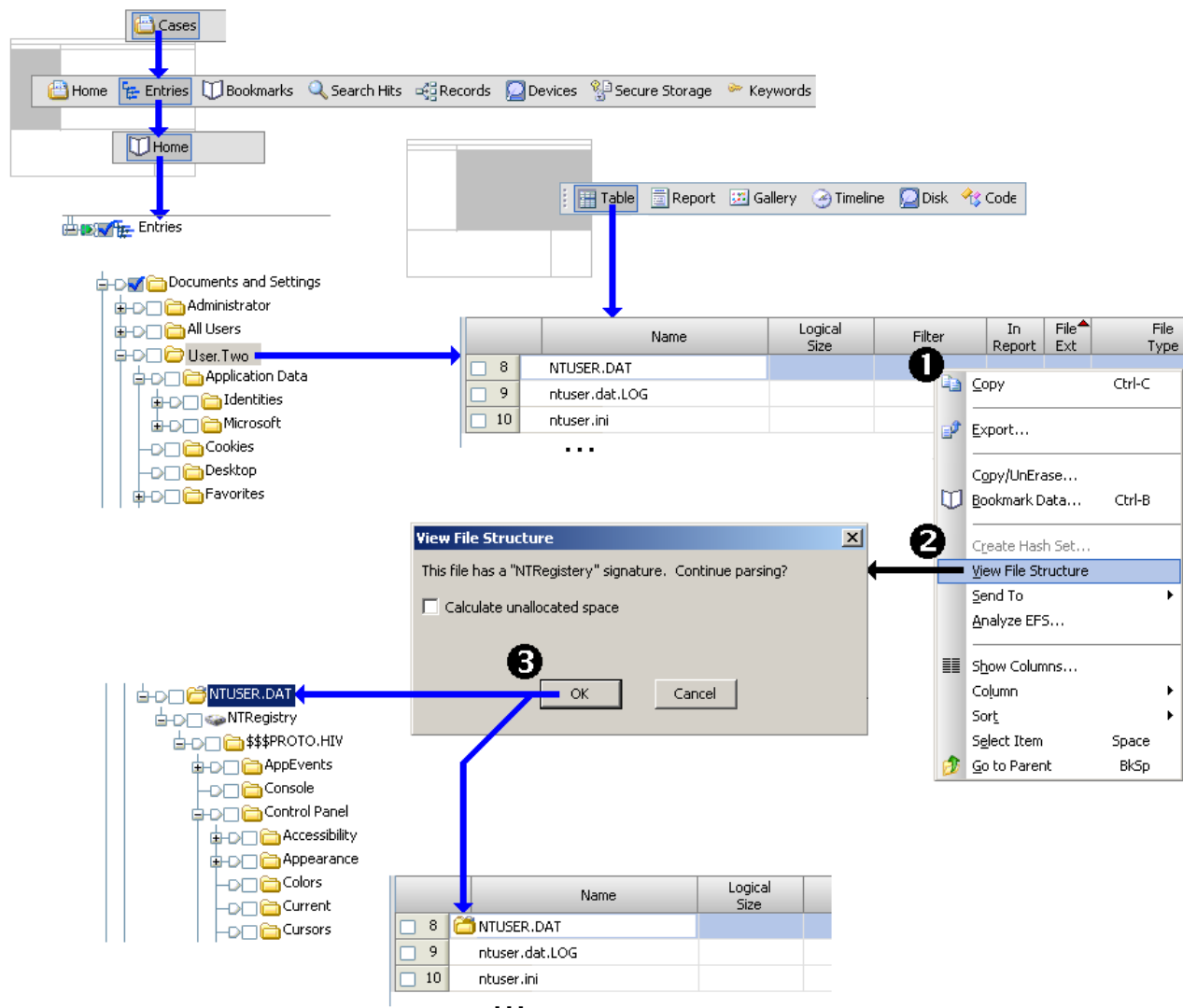
The Windows registry contains valuable data that provides a great deal of information about the setup of the subject computer. Registry files of Windows 95, 98, ME, NT 4.0, 2000, and XP computers can be mounted.

Windows 95, 98, and ME computers have two registry files. They are located in the system root folder, which is normally `C:\Windows`. The file names are `system.dat` and `user.dat`.

Windows NT 4.0, 2000, and XP divide the registry into four separate files. They are:

- Security
- Software
- SAM
- System

These files are stored in `C:\%SYSTEMROOT%\system32\config\`.



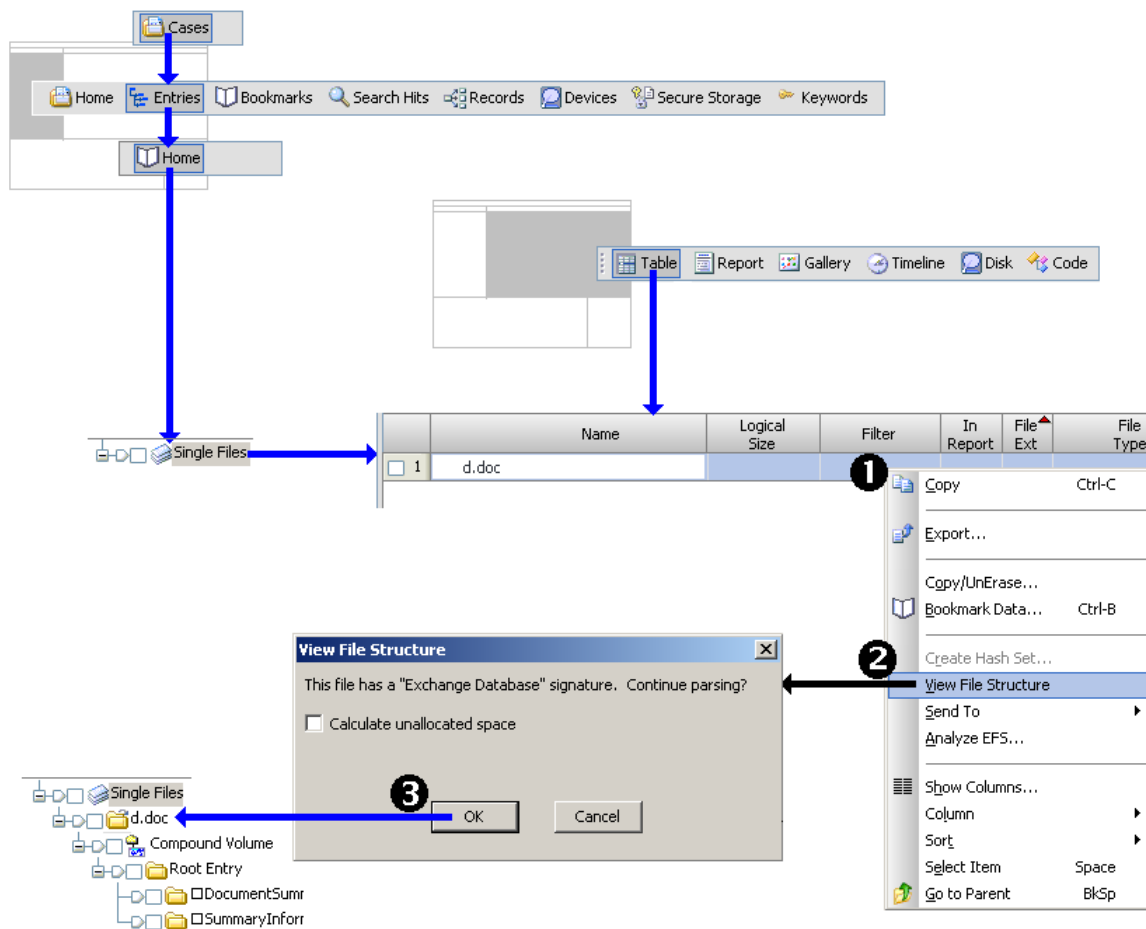
*To view or mount registry files:*

1. Navigate to the registry file you want to view or mount.
2. Continue with step 2 of Viewing File Structure.

The file structure of the registry file displays, and component files or layers in the compound volume folder can be opened and displayed in the view of your choice.

## Viewing OLE Files

OLE is Microsoft's Object Linking and Embedding technology used in the Microsoft Office suite of products. For example, OLE allows an Excel spreadsheet to be seamlessly embedded into a Word document. Microsoft Office documents that use this technology are layered compound files.



### To view or mount OLE files

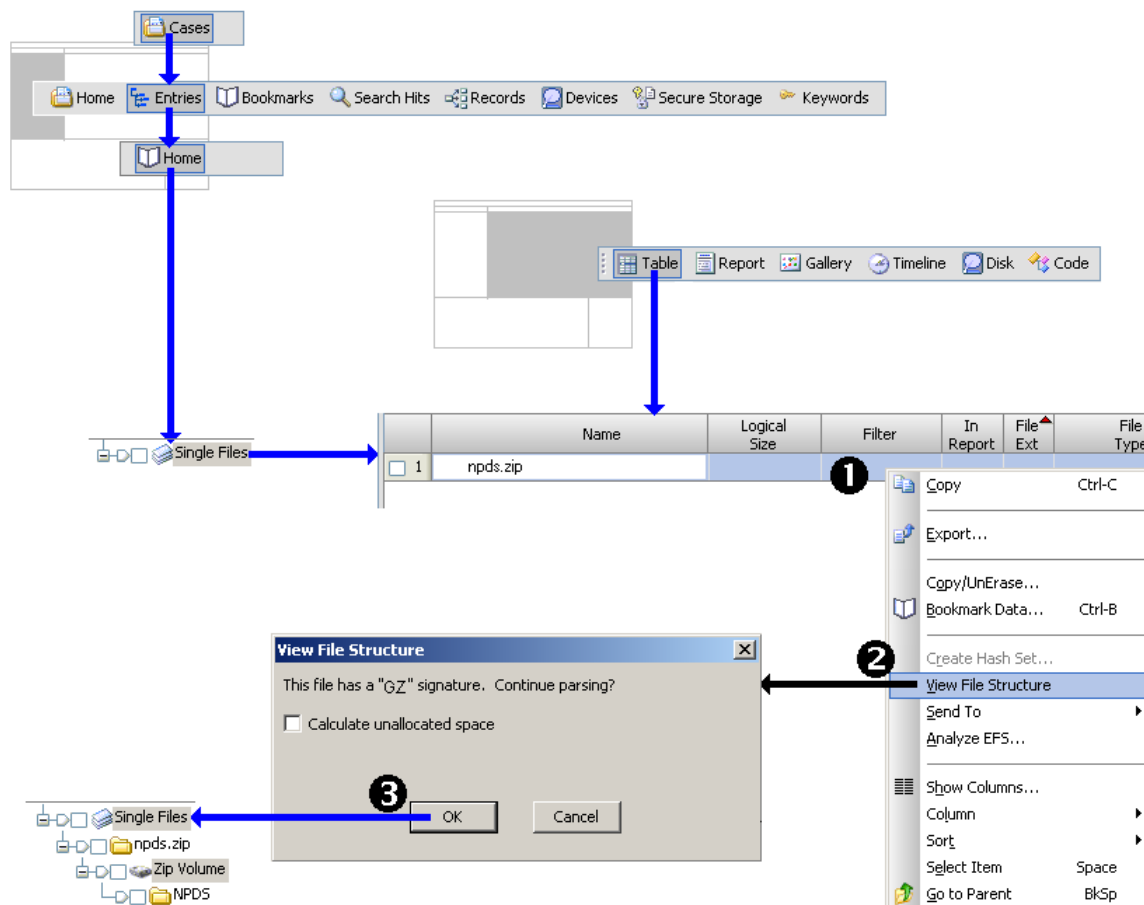
1. Navigate to the OLE file you want to view or mount.
2. Continue with step 2 of Viewing File Structures.

The file structure of the OLE file displays, and component files or layers in the compound volume folder can be opened and displayed in the view of your choice.

## Viewing Compressed Files

EnCase applications can mount compressed files including WinZip (.zip) GZip (.gz) and Unix tape archive (.tar) files. The contents are displayed as long as the container is not password protected.

Only the modified date and times are shown on .gz and .tar files, as the compression processes do not store any other dates or times. GZip files are not labeled by name, only by their content file type and a .gz extension. For example, decompressing the file document.doc.gz displays the uncompressed .doc file.



*To view or mount compressed files:*

1. Navigate to the compressed file you want to view or mount.
2. Continue with step 2 of Viewing File Structure.

The file structure of the compressed file displays, and component files or layers in the compound volume folder can be opened and displayed in the view of your choice.

## Viewing Lotus Notes Files

Lotus Notes versions 5, 6, 6.5, and 7 provide NSF support, which allows you to view email, appointments, and journal entries.

1. Navigate to the .NSF file you want to view or mount.
2. As needed, select **Calculate unallocated space**, then select **Find deleted content**.
3. Continue with step 2 of Viewing File Structure.

The file structure of the email (.nsf) file displays, and component files or layers in the compound volume folder can be opened and displayed in the view of your choice. Notice the icon for the compound email file looks like a disk drive, and no compound volume indicator is added to the icon after it is parsed.

## Viewing MS Exchange Files

MS Exchange 2000/2003 .edb support provides the ability to view mailboxes and emails.

1. Navigate to the .edb file you want to view or mount.
2. As needed select **Calculate unallocated space**, then select **Find deleted content**.
3. Continue with step 2 of Viewing File Structure.

The file structure of the email (.edb) file displays, and component files or layers in the compound volume folder can be opened and displayed in the view of your choice. Notice that the icon for the compound email file looks like a disk drive, and no compound volume indicator is added to the icon after it is parsed.

## Exchange Server Synchronization

The MS Exchange Server stores email messages in an EDB file on a server with a corresponding log file named E##.log. The log file is where Exchange stores data to be committed to the EDB file. In older Server versions, there is also a corresponding .stm file. When the log file contains data that has not been committed to the EDB file, the EDB file is in an inconsistent or "dirty" state. EnCase is unable to parse inconsistent EDB files.

To synchronize the structure, do the following:

1. Stop the Exchange Server service (if running).
2. Turn Exchange Server file shadowing on.
3. Copy the following folders from the Exchange Server to an EnCase working folder:
  - ☐ The bin directory to get the eseutil.exe program.
  - ☐ The mdbdata directory which contains both the private and public EDB files.

4. Start eseutil.exe using the Windows **Start→Run→**[location]\eseutil command.
5. Use the eseutil.exe command line tool to check the consistency of the state field as follows:
  - ☐ [file location]\eseutil /mh [filepath]priv1.edb
  - ☐ [file location]\eseutil /mh [filepath]pub1.edb

If the EDB file is in an inconsistent state, first try to recover, as follows:

- ☐ "C:\Exchange\BIN\Eseutil.exe" /r E##. Click **Yes** to run the repair.

Note that the three-character log file base name represents the first log file.

Files are sequentially named, with E##.log being the first log file.

Run a check (step 5) on the resulting EDB file. If the file is still in an inconsistent state, attempt to repair the EDB file. This may result in the loss of some data currently in the .log files. Run the repair as follows:

- ☐ "C:\Exchange\BIN\Eseutil.exe" /p

For additional information on the Eseutil program, read the Microsoft article at <http://support.microsoft.com/kb/272570/en-us> (<http://support.microsoft.com/kb/272570/en-us>).

## Cleaning an EDB Database

The MS Exchange Server stores email messages in an EDB file on a server with a corresponding log file named E##.log. The log file is where Exchange stores data to be committed to the EDB file. In older Server versions, there is also a corresponding .stm file. When the log file contains data that has not been committed to the EDB file, the EDB file is in an inconsistent or "dirty" state. EnCase is unable to parse inconsistent EDB files.

When an EDB file is dirty, there are several tests that can be run on it to determine whether the files are merely out of sync, or are in fact corrupt and unusable.

The next section discusses these tests.

## Testing an EDB File

This section describes how to determine whether the EDB database is in a usable state.

Acquire the EDB database, including the entire bin and mdbdata folders prior to running these checks. Make sure all codepages are installed on your computer.

The mdbdata folder contains the public and private databases and the transactional logs which are most important when cleaning a database. The BIN folder contains eseutil.exe.

1. Run `eseutil.exe` from **Windows→Start→Run**.
2. Use the `eseutil.exe` command line tool to check the consistency of the state field as follows:
  - ☐ `[file location]\eseutil /mh [filepath]priv1.edb`
  - ☐ `[file location]\eseutil /mh [filepath]pub1.edb`

If the EDB file is in an inconsistent state, first try to recover, as follows:

- ☐ `"C:\Exchange\BIN\Eseutil.exe" /r E##`. Click Yes to run the repair.

Note that the three-character log file base name represents the first log file.

Files are sequentially named, with `E##.log` being the first log file.

Run a check (step 2) on the resulting EDB file. If the file is still in an inconsistent state, attempt to repair the EDB file. This may result in the loss of some data currently in the .log files. Run the repair as follows:

- ☐ `"C:\Exchange\BIN\Eseutil.exe" /p`

For additional information on the Eseutil program, read the Microsoft article at <http://support.microsoft.com/kb/272570/en-us> (<http://support.microsoft.com/kb/272570/en-us>).

## Recovering a Database

These instructions describe how to recover from a dirty EDB database.

Enter these commands: `"C:\Exchange\BIN\Eseutil.exe" /r E## [options]`

Options include:

- ☐ `/l<path>` - location of log files
- ☐ `/s<path>` - location of system files
- ☐ `/i<path>` - ignore mismatched/missing database attachments
- ☐ `/d<path>` - location of database files
- ☐ `/o` - suppress logo

## Repairing a Database

These instructions describe how to repair an EDB database.

Enter these commands: `"C:\Exchange\BIN\Eseutil.exe" /p <database name> [options]`

Options include:

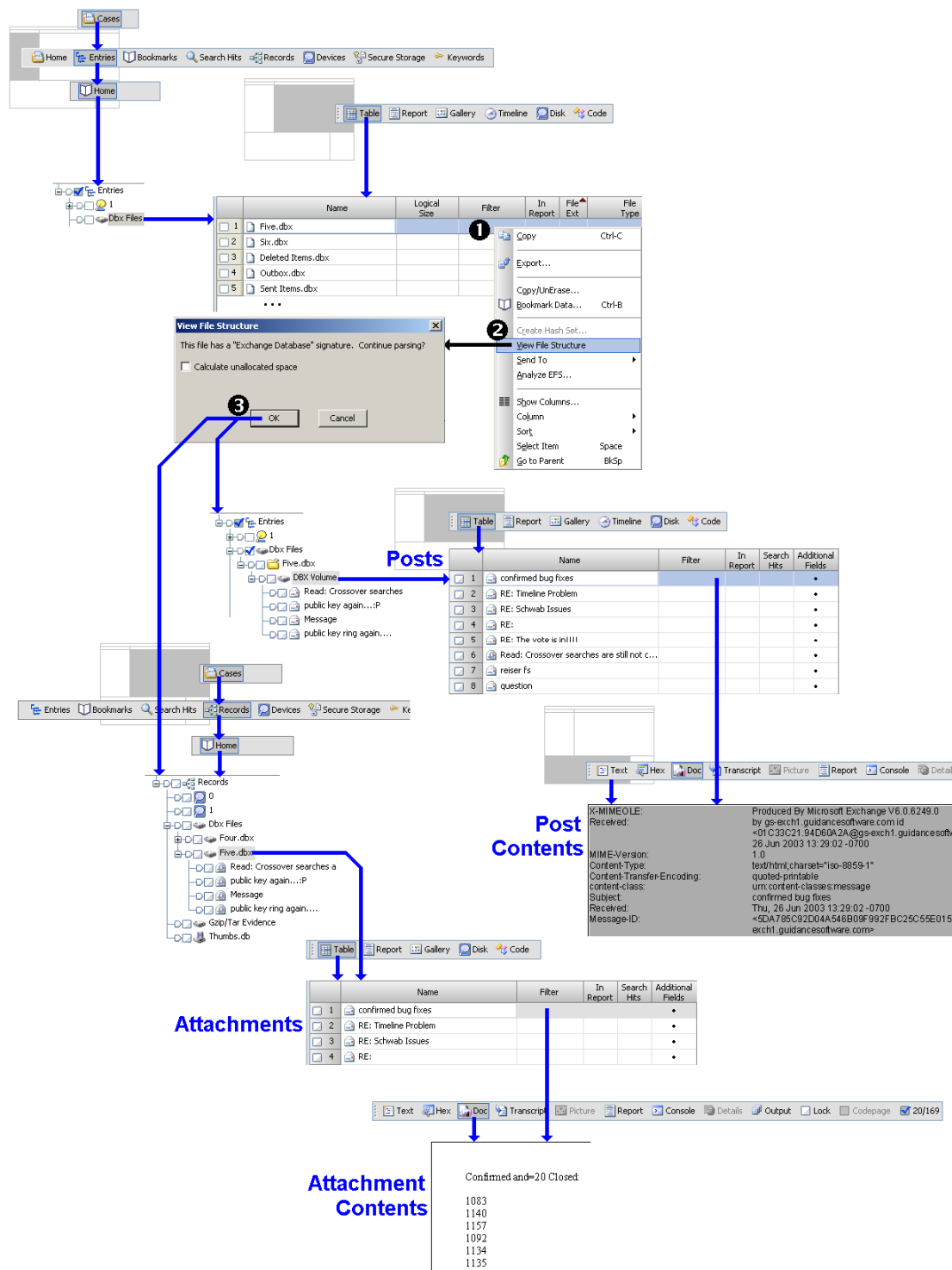
- ☐ `/s <file>` - set streaming file name
- ☐ `/i` - bypass the database and streaming file mismatch error
- ☐ `/o` - suppress logo
- ☐ `/createstm` - create empty streaming file if missing
- ☐ `/g` - run integrity check before repairing
- ☐ `/t <database>` - set temporary database name
- ☐ `/f <name>` - set prefix to use for name of report files



## Viewing Outlook Express Email

EnCase applications can read Outlook Express .dbx files. After the file structure is parsed, the Entries and Records tables in the Table pane lists individual emails by their subject line. The records table pane lists the attachments. The View pane displays the contents of the selected email or attachment.

Deleted emails and attachments can be retrieved from unallocated clusters.



1. Navigate to the .dbx file you want to view or mount.
2. As needed select Calculate unallocated space, then select Find deleted content.
3. Continue with step 2 of Viewing File Structure.

The file structure of the email (.dbx) file displays, and component files or layers in the compound volume folder can be opened and displayed in the view of your choice. Notice that the icon for the compound email file looks like a disk drive, and no compound volume indicator is added to the icon after it is parsed.

## Viewing MS Outlook Email

The process of mounting Outlook .pst files is identical to that of Outlook Express as previously described. When EnCase applications mount an Outlook .pst file, messages are viewable by clicking on the PR\_Body file and selecting the Text tab in the View pane. Because the text is likely Unicode, apply a unicode text style to make it easier to read.

When expanded, the top level (or top root) of the .pst file directory contains multiple folders, including

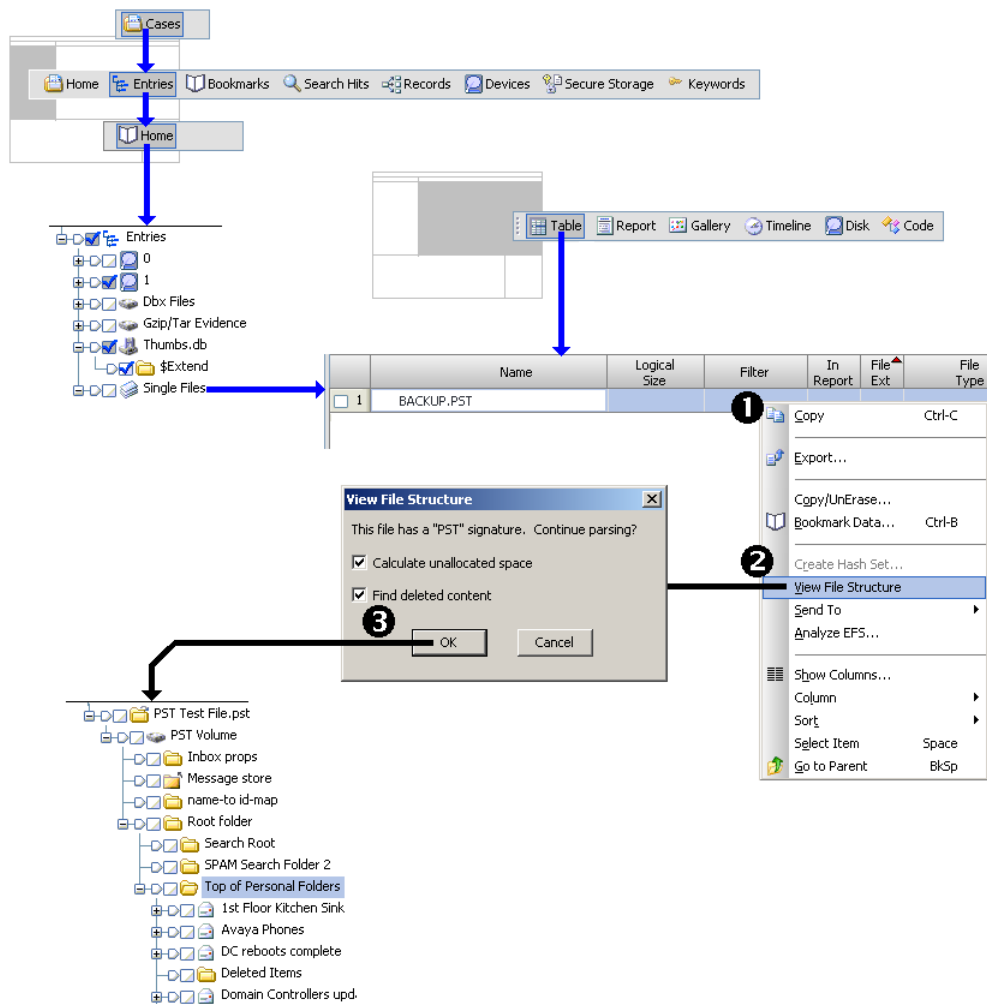
- Inbox props (properties)
- Message store (storage, containing the PR\_PST\_PASSWORD file and other IDs)
- Name-to-id-map
- Root folder

The Root folder contains:

- Search Root (reserved for future use)
- Top of Personal Folders, containing the Inbox, Sent Items, and Deleted Items

Each .pst email message file appears as a folder with all message properties within the folder as well as any attachments.

Many of the fields within the .pst mail folder are duplicated, which is part of the .pst format. If a keyword is a match within a certain field, it is duplicated in the secondary field as well. Created, written and modified dates are set by the email messages. Outlook calendar entries (created, written and modified dates) are set by the calendar applications.



To view or mount an MS Outlook email:

1. Navigate to the .pst file you want to view or mount.
2. As needed, select **Calculate unallocated space**, then select **Find deleted content**.
3. Continue with step 2 of Viewing File Structure.

The file structure of the email file displays, and component files or layers in the compound volume folder can be opened and displayed in the view of your choice. Notice that the icon for the compound email file looks like a volume after it was mounted.

## Viewing Macintosh .pax Files

You can parse Macintosh .pax files formatted with the cpio file format can be parsed using View File Structure.

1. Navigate to the .pax file you want to view or mount.
2. As needed, select **Calculate unallocated space**, then select **Find deleted content**.

3. Continue with step 2 of Viewing File Structure.

The file structure of the email (.PAX) file displays, and component files or layers in the compound volume folder can be opened and displayed in the view of your choice. Notice that the icon for the compound email file looks like a disk drive, and no compound volume indicator is added to the icon after it is parsed.

## Viewing Windows Thumbs.db

EnCase applications support parsing the Windows thumbs.db cache for images. Once mounted the thumbnail cache volume and the version appear. V2 thumbnails are in bitmap format, whereas later versions are modified .pngs. The Root Entry folder contains:

- the catalog file of cached thumbnail names
- their full path
- the cached images themselves

Thumbs.db also contains a record of the image's Last Written date.

The screenshot illustrates the steps to view a Windows Thumbs.db file in EnCase:

- File List:** The main table lists files in the Root Entry folder. The file 'Thumbs98.db' is selected.

	Name	Filter	In Report	File Ext	File Type	File Category	Signature
14	\$Secure:\$SDS						
15	\$UpCase						
16	Thumbs98.db				Database	Database	
17	Thumbs98.db'encr...						
18	Thumbs_xp.db				ase Database	Database	
19	Thumbs_2k.db						
20	MFT Allocation Bitmap						
21	Unallocated Clusters						

- Context Menu:** A right-click menu is open over 'Thumbs98.db', with 'View File Structure' selected.
- View File Structure Dialog:** A dialog box appears with the message: 'This file has a "Structured" signature. Continue parsing?' and an unchecked checkbox for 'Calculate unallocated space'. The 'OK' button is clicked.
- Thumbnail Cache Volume (V2):** The file tree on the left shows 'Thumbnail Cache Volume(V2)' expanded, with 'Root Entry' selected.
- File List (Thumbnail Cache Volume):** The main table now shows the contents of the Root Entry folder, which are image files.

	Name	Filter	In Report	File Ext	File Type	File Category
1	D:\matt\Zips\William Schimmel\schim05...			.jpg	JPEG	Picture
2	D:\matt\Zips\William Schimmel\schim01...			.jpg	JPEG	Picture
3	D:\matt\Zips\William Schimmel\Dolphin...			.jpg	JPEG	Picture
4	D:\matt\Zips\William Schimmel\DCOTE....			.jpg	JPEG	Picture
5	D:\matt\Zips\William Schimmel\Concep...			.jpg	JPEG	Picture
6	Catalog					
7	D:\matt\Zips\William Schimmel\COTER....			.jpg	JPEG	Picture

- Preview:** The bottom window shows a preview of the selected image file, which is a picture of three white bears.

To view or mount a Windows thumbs.db file:

1. Navigate to the desired file in the thumbs.db.
2. Right-click the file, then click **View File Structure**.
3. As needed, select **Calculate unallocated space**.
4. Continue with step 2 of Viewing File Structure.

The file structure of the email (.PST) file displays, and component files or layers in the compound volume folder can be opened and displayed in the view of your choice. The compound volume indicator is added to the thumbs.db folder after it is parsed.

## America Online .art Files

EnCase applications support America Online .art format images in the Picture and Gallery tabs. .art support requires installation of the Internet Explorer AOL Support module on the examiner machine. The installer is available to download from

<http://www.microsoft.com/technet/prodtechnol/windows2000serv/downloads/aolsupp.msp>  
(<http://www.microsoft.com/technet/prodtechnol/windows2000serv/downloads/aolsupp.msp>).

This installs the files:

- Jgaw400.dll
- Jgdw400.dll
- Jgmd4.dll
- Jgpl400.dll
- Jgsd400.dll
- Jgsh400.dll

---

This update is only required for Windows 2000. Newer operating systems do not need this patch.

---

View the file in the picture or gallery view as any other image file.

---

Occasionally corrupt .art files can cause EnCase to stop responding. If this occurs, try lowering the invalid picture timeout setting (In Global Options) or simply disable "Enable ART and PNG image display", also in Global options.

---



## Viewing Office 2007 Documents

Microsoft's Office 2007 documents are stored in the Office Open XML file format. This is a .zip file of various XML documents describing the entire document. The EnCase® suite supports viewing Office 2007 Word, Excel and PowerPoint document files.

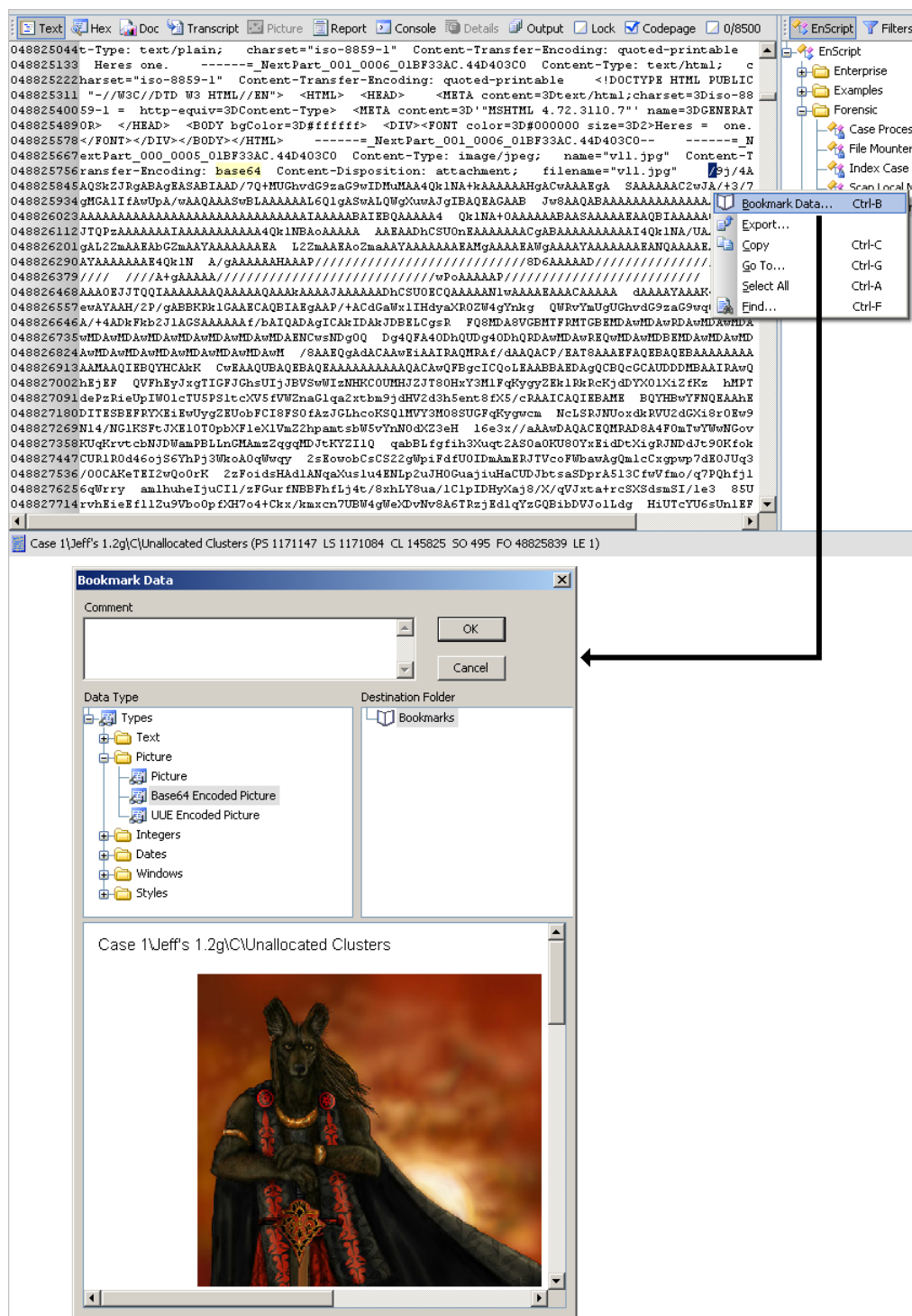
EnCase extracts text from Word, Excel, and PowerPoint documents. It parses Excel worksheet values as well.

Right-click the desired file, then click View File Structure.

1. Navigate to an XML file containing child nodes.
2. The viewer displays text from the document.

## Viewing Base64 and UUE Encoded Files

EnCase applications automatically display Base64 and UUE encoded attachments when the mail file is mounted. For these encoded files, you either perform a keyword search for Base64 or UUE, or you notice that a file is encoded as such.



### To view Base64 and UUE encoded files

1. Highlight the file in the Table pane, so that the content of the file appears in the Text tab of the View pane.
2. Highlight the first character, right-click, and click **Bookmark Data**.

The Bookmark Data dialog appears.

3. In Data Type, select either **Base64-Encoded Picture** or **UUE Encoded Picture**.

The picture displays in the Contents pane.

## NTFS Compressed Files

EnCase decompresses, views and searches NTFS compressed files in real time, or in an on-the-fly manner by detecting a compressed file, then automatically preparing it for analysis.

The investigator can view uncompressed file data in the Disk tab of the Table pane.

## Gallery Tab

The Gallery tab provides a quick and easy way to view images stored on the subject media. This includes all images purposely stored as well as those inadvertently downloaded from the Web.

You can access all images within a highlighted folder, highlighted volume, or the entire case. If a folder is highlighted in the Tree pane, all files in the folder are displayed in the Table pane.

Clicking a folder's **Set Include** selects all files in that folder and files in any of its subfolders.

Once selected on the Table pane, any images in the selected files display in Gallery tab.

You can bookmark images in the Gallery tab and display them in the report.

The Gallery tab displays files based on their file extension by default. For example, if a .jpg file has been renamed to .dll, it WILL NOT be displayed in the Gallery tab until you run a ***Signature Analysis*** (on page 327). Once the signature analysis recognizes that the file was renamed and that the file is actually an image, it is displayed in the Gallery tab.

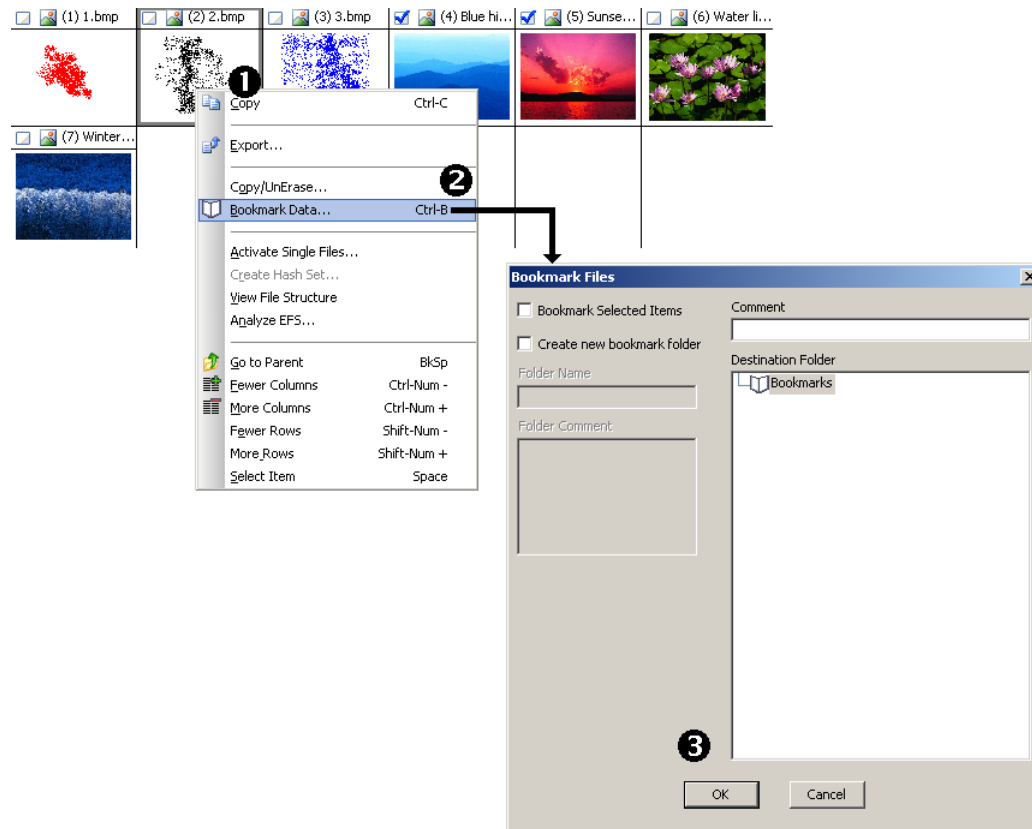
EnCase applications include built-in crash protection, which prevents corrupted graphic images from appearing in the Gallery or Picture tab. The corrupt images are stored in cache so that they are recognized the next time they are accessed. No attempt is made to display them. These images are cached at the case level so they do not attempt to display in that case file again until you run a signature analysis.

You can clear the cache. This setting appears on the shortcut menu only if a corrupt image is encountered. The timeout defaults to 12 seconds for the thread trying to read a corrupt image file. You can modify the timeout on the Global tab of the Options dialog.

## Bookmarking an Image

You can bookmark images on the Gallery tab of the Table pane.

Figure 31



1. Select the desired image or images.
2. Right-click the highlighted image, and click **Bookmark File**.

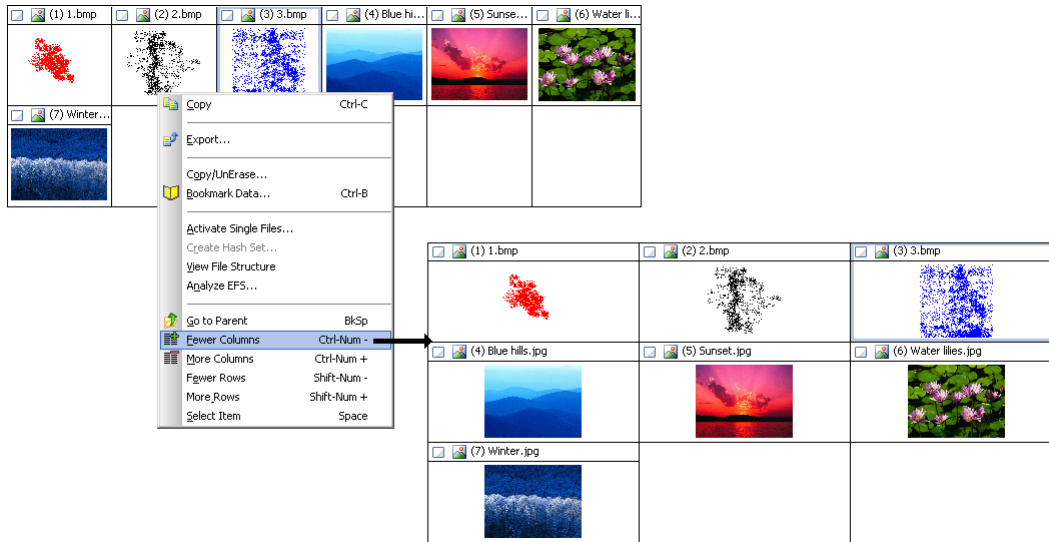
The Bookmark Files dialog appears.

3. Modify the settings as needed, and click **OK**.

The image or images are bookmarked. They are in the Table pane when the Bookmark tree displays.

## Reducing the Number of Images Per Row

You can reduce the number of images displayed in a row in the Gallery tab.

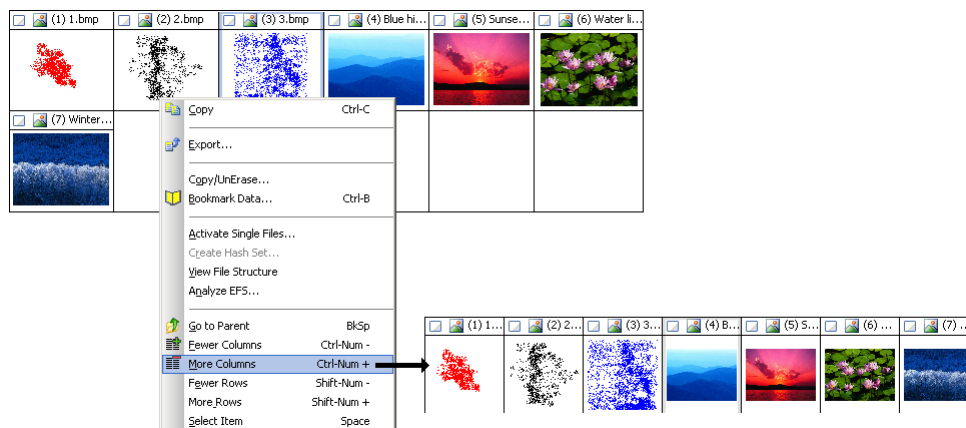


*To reduce the number of images displayed in a row in the gallery tab*

- Right-click on any image on the Gallery tab, and click **Fewer Columns**.

## Increasing the Number of Images Per Row

You can increase the number of images displayed per row in the Gallery tab.



*To increase the number of images displayed per row in the gallery tab*

- Right-click on any image in the Gallery tab, then click **More Columns**.

## Clearing the Invalid Image Cache

The program includes built-in crash protection, which prevents corrupted graphic images from appearing in Gallery or Picture view. The corrupt images are stored in a cache so that EnCase recognizes them the next time they are accessed, and does not attempt to display them. These images are cached at the case level so that the images do not attempt to display in that case file again.

Before you can clear the cache, the Cases tree displays in the Cases tab of the Tree pane. You can clear the cache only if a corrupt image is encountered.

1. Right-click on the Cases root object in the Cases Tree.
2. Click **Clear invalid image cache**.

## Lotus Notes Local Encryption Support

EnCase can decrypt a local Lotus Notes user mailbox (NSF file suffix). The local mailbox is a replica of the corresponding encrypted mailbox on the Domino server.

Each Domino server user has a corresponding NSF file representing that user's mailbox in 8.3 format. The default path is <Domino Installation Folder>\Data\Mail\<user>.nsf. The Lotus Notes client is set up to use the local mailbox. Synchronization between the local and server mailboxes occurs according to a replication schedule determined by the Domino administrator.

Encryption of the local mailbox is not mandatory but it is advisable, because without encryption a person familiar with the NSF file structure could read email without needing Lotus Notes.

Encryption occurs at block level.

## Determining Local Mailbox Encryption

Look in the header (the first 0x400 bytes) at offset 0x282. If the byte is 0x1, the mailbox is locally encrypted.

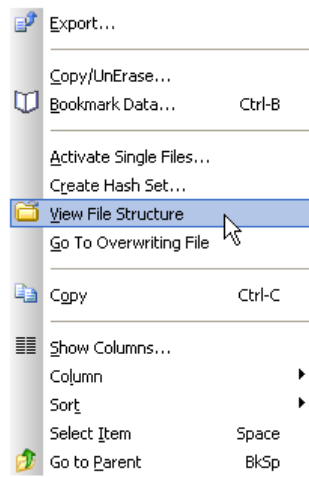
```

00000240| 04 01 00 00 00 00 01 00 00 00 00 00 00 00 00 00 | .....
00000250| 00 00 04 00 04 00 04 00 20 00 00 00 80 00 00 00 | .....
00000260| 00 F8 00 00 00 80 00 00 F4 01 05 00 62 00 64 00 | .....b.d.
00000270| 00 50 00 00 F5 F4 00 00 00 50 00 00 45 F5 00 00 | .P.....P..E...
00000280| 00 00 01 81 00 00 55 00 00 00 C5 23 7B F1 86 03 | .....U...#{...
00000290| 00 00 B1 1F 63 00 C2 72 25 00 04 02 00 00 00 00 | ....c..r%.....
000002A0| 00 00 00 00 00 00 6D 4A CB 5D 00 00 00 00 00 00 | .....mJ.].....
000002B0| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
000002C0| 01 00 00 00 00 20 00 00 00 00 00 4A 00 00 00 00 | .....J.....
000002D0| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....

```

## Parsing a Locally Encrypted Mailbox

1. Obtain the corresponding ID file from the Domino server. All user ID files are backed up on the server either on disk as a file or in the Domino directory as an attachment to email.
2. Parse it using **View File Structure**, so that the private key is inserted in Secure Storage.





## Encrypted Block

The example below shows an encrypted block at offset 0x22000:

Memory 1															
Address: 0x02C8CB44															
Columns: 16															
0x02C8CB44	5e	cc	65	dc	2e	f0	17	f1	da	73	d7	b7	8c	a7	48 00
0x02C8CB54	b7	68	05	01	7e	dd	f5	f7	ab	a9	97	94	08	f9	fc d2
0x02C8CB64	94	04	69	82	64	53	4a	c1	d2	ca	e9	cd	0a	f0	8a 15
0x02C8CB74	7d	ae	1c	21	d3	c8	c4	63	75	f5	16	04	de	1b	e0 7f
0x02C8CB84	26	bc	14	b6	c3	f5	b2	07	ca	bb	96	f0	d2	f3	2b 09
0x02C8CB94	d4	b7	aa	7a	68	fa	86	2b	5d	f6	d6	0e	f3	0e	7a 88
0x02C8CBA4	2d	49	fd	6c	59	66	b2	0c	9c	ef	12	df	82	ba	79 7f
0x02C8CBB4	fd	48	a5	87	99	ca	9a	26	0a	7b	87	05	c7	7f	b1 e9
0x02C8CBC4	77	e8	a2	9f	bc	1d	c9	c2	d1	1c	8e	f5	4e	72	e6 df
0x02C8CBD4	cc	99	92	62	bb	a2	65	ed	bb	d3	68	a7	e2	50	7f da
0x02C8CBE4	84	12	73	f6	72	f2	8f	61	23	5c	be	e6	54	47	07 85
0x02C8CBF4	78	61	d4	42	92	02	72	be	d0	c3	01	60	04	f6	22 04
0x02C8CC04	3a	14	d3	22	a1	f6	23	d0	cd	48	85	84	c4	ec	15 32
0x02C8CC14	d0	ce	f2	7a	f1	3d	fb	60	d5	6f	26	ed	82	0d	85 fb
0x02C8CC24	24	92	0d	15	bd	b2	39	e7	7c	58	3e	a3	9c	c1	0e 61
0x02C8CC34	b5	da	42	49	08	00	e7	b6	04	48	05	2e	63	bd	85 c9
0x02C8CC44	88	e8	a3	d2	a7	97	8b	25	ab	a8	b0	9e	c0	d8	99 75
0x02C8CC54	e2	0e	09	4f	c9	e0	9b	e2	2f	b4	d3	68	b2	07	69 f8
0x02C8CC64	8b	99	07	68	b2	83	20	be	79	cb	8d	05	1a	be	fe b3
0x02C8CC74	9d	46	4b	ae	9c	37	7a	8b	8f	33	57	be	7d	96	72 92
0x02C8CC84	ff	72	37	f0	d2	e3	a4	d8	7a	8d	a2	b0	d2	d1	16 3d
0x02C8CC94	13	6c	8b	79	93	af	96	20	34	ca	50	fe	f2	d9	f6 3e
0x02C8CCA4	cb	5b	ae	75	9b	41	07	ac	34	cf	9a	52	82	f5	05 d4
0x02C8CCB4	f7	04	92	25	92	96	91	c1	54	ba	60	e2	6c	8a	8c ab
0x02C8CCC4	90	97	6b	bc	88	35	32	ac	07	13	64	dd	2c	b2	8d 8c
0x02C8CCD4	f6	7b	38	39	82	dd	42	20	53	04	b4	9c	f9	b6	f2 b9
0x02C8CCE4	cb	6b	f2	84	c1	8d	16	dc	39	3a	87	41	56	a7	a1 01
0x02C8CCF4	23	ab	5e	7e	f2	02	b6	8a	5a	25	41	d6	d7	4d	51 a8
0x02C8CD04	15	51	a2	dd	24	31	2e	fe	30	b9	5e	74	50	f3	07 ee
0x02C8CD14	99	1d	02	24	d3	05	be	7d	95	1d	38	97	d9	6f	ad b9
0x02C8CD24	e7	01	fe	b5	17	6a	bc	73	9c	80	82	4b	31	b0	dd 88
0x02C8CD34	38	2f	5c	86	cb	ce	e3	0c	80	34	8d	b4	4b	d2	99 e2
0x02C8CD44	3f	e3	b7	38	6d	b2	10	e1	ac	d6	de	98	9a	11	f4 e6

The decryption algorithm uses a seed that is based on the basic seed from the header and the block offset.

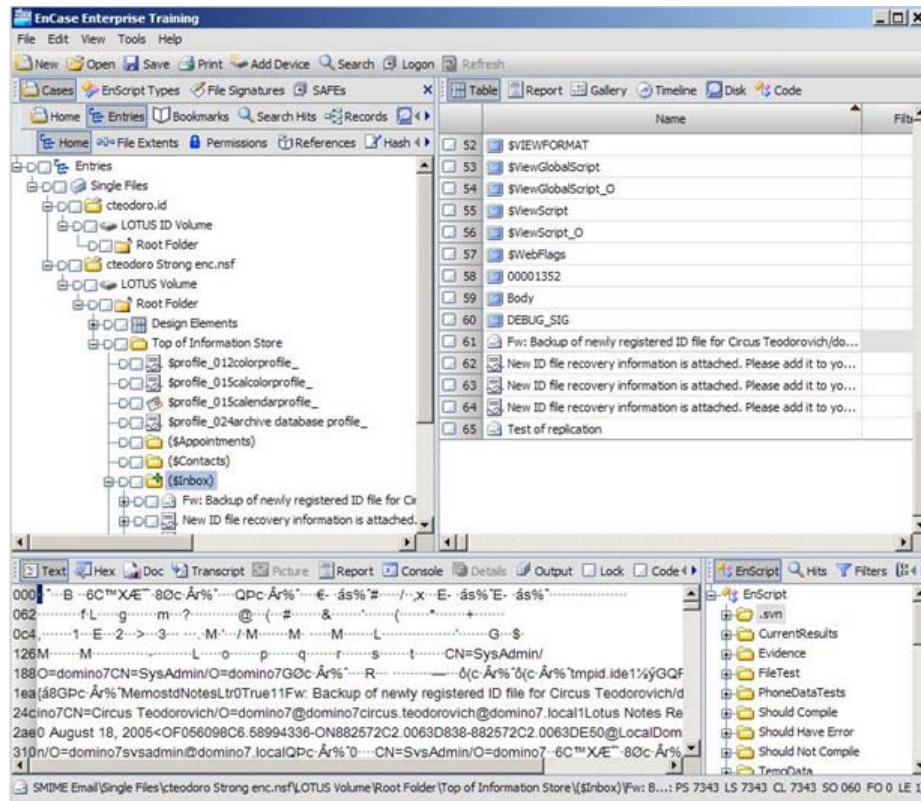
## Decrypted Block

Here is an example of a decrypted object map at offset 0x22000:

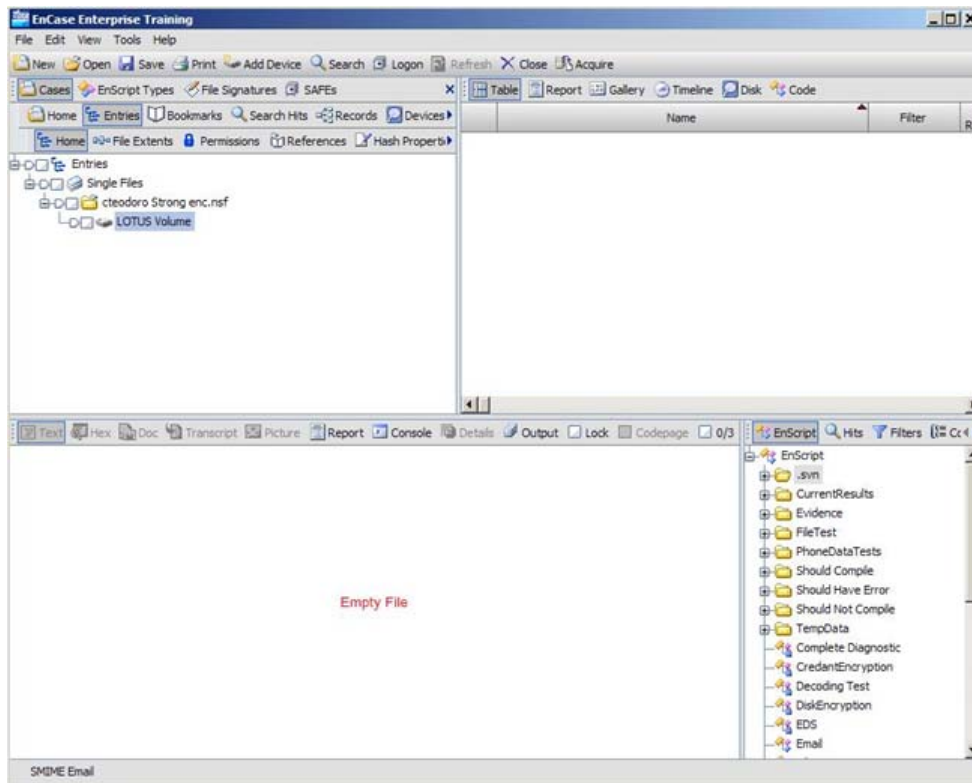
Memory 1															
Address: 0x02C8CB44		{a}		Columns: 16											
0x02C8CB44	06	20	00	00	00	00	06	01	00	00	00	00	00	00	00
0x02C8CB54	00	01	89	a6	ff	ff	00	00	00	00	00	00	00	00	00
0x02C8CB64	4c	05	00	00	00	00	00	ec	04	00	00	00	00	00	00
0x02C8CB74	4d	02	00	00	00	00	00	18	02	00	00	00	00	00	00
0x02C8CB84	01	00	00	80	01	08	00	00	17	02	00	00	00	00	00
0x02C8CB94	1d	02	00	00	00	00	00	01	00	00	80	02	00	00	00
0x02C8CBA4	1e	02	00	00	00	00	00	01	00	00	80	03	00	00	00
0x02C8CBB4	02	00	00	80	02	08	00	00	02	00	00	80	03	08	00
0x02C8CBC4	02	00	00	80	04	08	00	00	02	00	00	80	05	08	00
0x02C8CBD4	02	00	00	80	06	08	00	00	02	00	00	80	07	08	00
0x02C8CBE4	02	00	00	80	08	08	00	00	02	00	00	80	0a	08	00
0x02C8CBF4	02	00	00	80	0e	08	00	00	02	00	00	80	0d	08	00
0x02C8CC04	02	00	00	80	0e	08	00	00	02	00	00	80	0f	08	00
0x02C8CC14	02	00	00	80	10	08	00	00	02	00	00	80	11	08	00
0x02C8CC24	02	00	00	80	12	08	00	00	02	00	00	80	13	08	00
0x02C8CC34	01	00	00	80	0b	08	00	00	01	00	00	80	0c	08	00
0x02C8CC44	03	00	00	80	01	08	00	00	03	00	00	80	02	08	00
0x02C8CC54	03	00	00	80	03	08	00	00	03	00	00	80	04	08	00
0x02C8CC64	03	00	00	80	05	08	00	00	03	00	00	80	06	08	00
0x02C8CC74	03	00	00	80	07	08	00	00	03	00	00	80	08	08	00
0x02C8CC84	03	00	00	80	09	10	00	00	03	00	00	80	0a	10	00
0x02C8CC94	03	00	00	80	0b	10	00	00	03	00	00	80	0c	10	00
0x02C8CCA4	03	00	00	80	0d	10	00	00	03	00	00	80	0e	10	00
0x02C8CCB4	03	00	00	80	0f	10	00	00	03	00	00	80	10	10	00
0x02C8CCC4	03	00	00	80	11	10	00	00	03	00	00	80	12	10	00
0x02C8CCD4	03	00	00	80	13	10	00	00	03	00	00	80	14	10	00
0x02C8CCE4	03	00	00	80	15	10	00	00	04	00	00	80	01	10	00
0x02C8CCF4	04	00	00	80	02	10	00	00	04	00	00	80	03	10	00
0x02C8CD04	04	00	00	80	04	10	00	00	04	00	00	80	05	10	00
0x02C8CD14	04	00	00	80	06	10	00	00	04	00	00	80	07	10	00
0x02C8CD24	04	00	00	80	08	10	00	00	04	00	00	80	09	10	00
0x02C8CD34	04	00	00	80	0a	10	00	00	04	00	00	80	0b	10	00
0x02C8CD44	04	00	00	80	0c	10	00	00	04	00	00	80	0d	10	00

## Locally Encrypted NSF Parsing Results

A successfully parsed locally encrypted NSF looks like this in Entry view:



If the corresponding ID file cannot be parsed successfully, the Secure Storage is not populated with the data needed to parse the locally encrypted NSF; thus, the Lotus volume is empty:



# Analyzing and Searching Files

- Signature Analysis 327
- EnScript Programming Language 337
- Hash Analysis 338
- File Hashing 339
- Hash Sets 340
- Keyword Searches 343
- Encode Preview 363
- Indexing 365
- Generating an Index 367
- Searching for Email 369
- App Descriptors 378
- Encryption Support 381
- EFS Files and Logical Evidence (LO1) Files 399

## Signature Analysis

There are thousands of file types, some of them are standardized. The International Standards Organization (ISO) and the International Telecommunications Union - Telecommunication Standardization Sector (ITU-T) are working to standardize different types of electronic data.

Typical graphic file formats such as JPEG (Joint Photographic Experts Group) have been standardized by both organizations. When a file type is standardized, a signature or recognizable header usually precedes the data. File headers are associated with specific file extensions. Signature analysis compares file headers with file extensions.

### File Signatures

File extensions are the characters (usually three) following the dot in a filename (e.g., signature.doc). They reveal the file's data type. For example, a .txt extension denotes a text file, while .doc connotes a document file. The file headers of each unique file type contain identifying information called a *signature*. All matching file types have the same header. For example, .BMP graphic files have **BM8** as a signature.

A technique often used to hide data is to attempt to disguise the true nature of the file by renaming it and changing its extension. Because a .jpg image file assigned a .dll extension is not usually recognized as a picture, comparing a file's signature, which doesn't change, with its extension identifies files that were deliberately changed. For example, a file with a .dll extension and a .jpg signature should pique an investigator's interest.

---

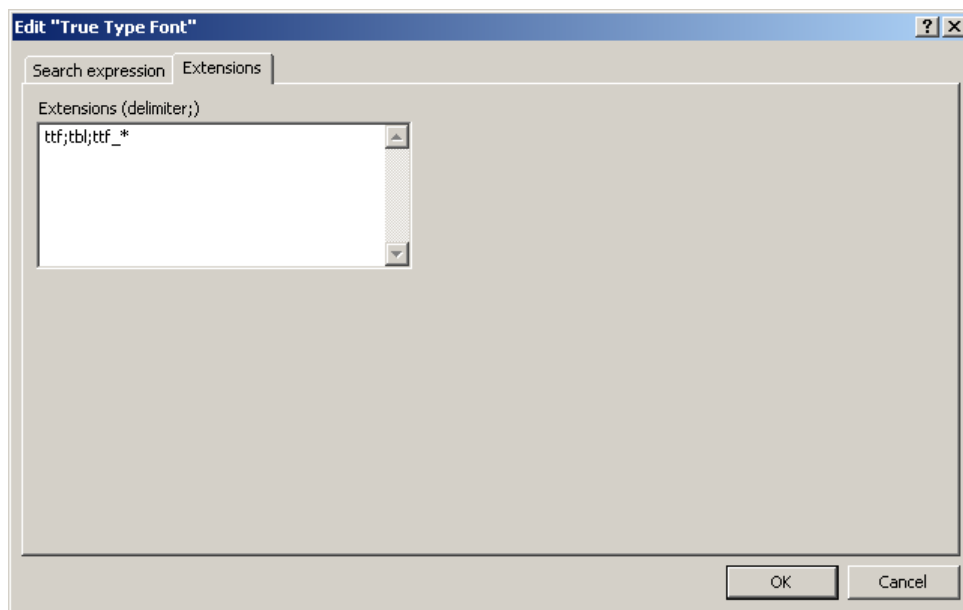
Note: The software performs the signature analysis function in the background.

---

## File Signatures with Suffixes

A shadow directory is a directory type containing symbolic links that point to real files in a directory tree. This is useful for maintaining source code for different machine architectures. You create a shadow directory containing links to the real source, which you usually mount from a remote machine.

The Vista operating environment uses shadow directories, and EnCase software's ability to suffix a file signature takes these directories into account. Extension suffixes are created by adding an underscore and asterisk to the end of the extension. The figure shows such a TrueType extension and suffix (ttf\_\*).



## Viewing the File Signature Directory

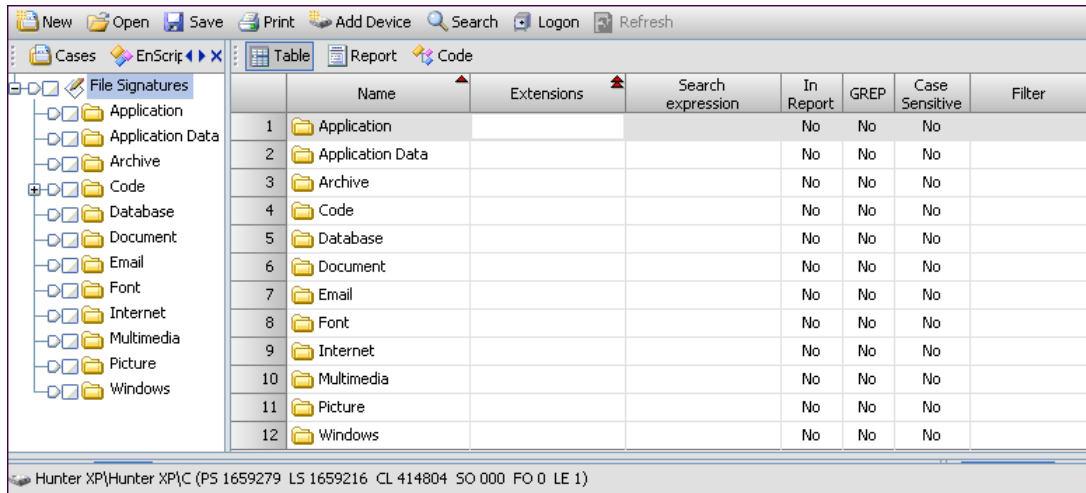
A File Signature table lists signatures the EnCase software recognizes. The table is organized into data types such as:

- database
- email
- Internet

To view the table:

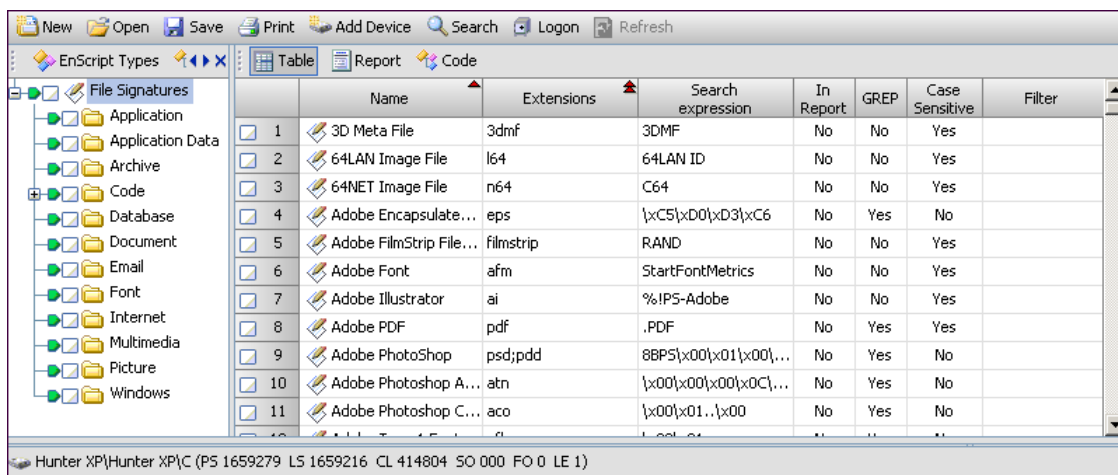
1. Select **View > File Signatures** from the menu bar.


A directory of file categories appears.



2. Select a folder from the Tree pane. The figure shows Document types selected.

A list of the file signatures in the case appears in the Table pane.



If **Set-Include**  is checked, all file signatures are listed.

The columns in the File Signature display are:

**Name** displays the file name associated with the signature.

**Search Expression** displays the string or GREP expression used to locate the file signature.

**GREP** is true if the search term is defined as a GREP expression.

**Case Sensitive** indicates whether the search term is case sensitive.



**Extensions** lists the three-letter file extensions.

You can add new or edit existing signatures.

## Adding a New File Signature

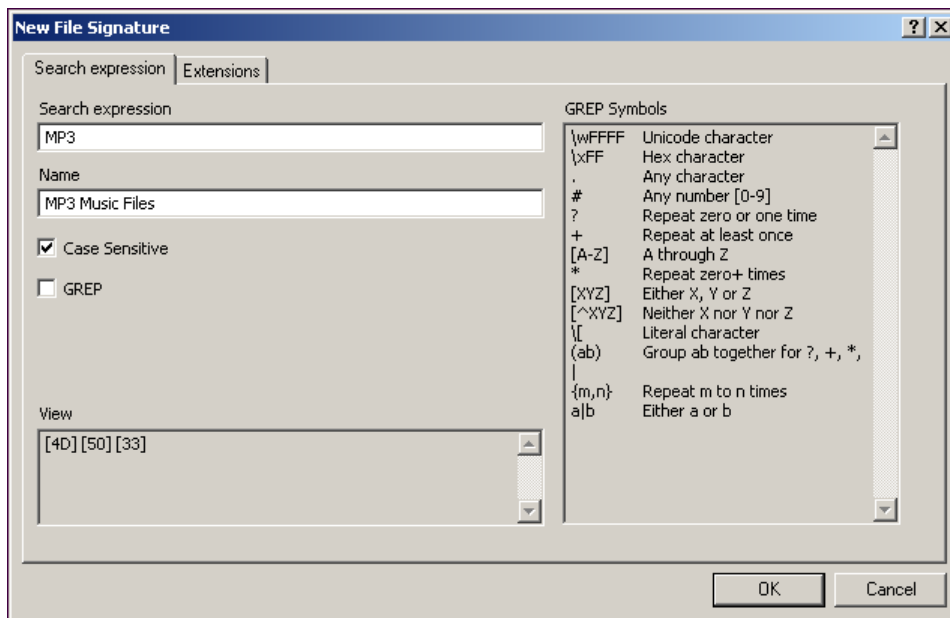
A file signature may not be in the table. Use this procedure to add a new one.

You need to know the file signature search expression. This is not necessarily the same as the three-letter file extension.

*To add a file signature to the table:*

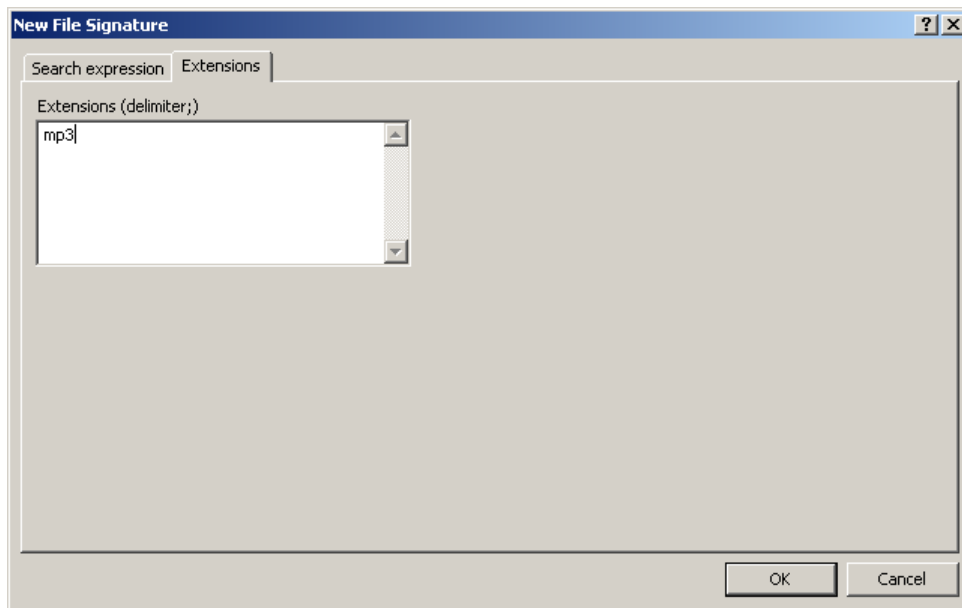
1. Click **View > File Signatures**. The file signature display appears.
2. Right-click a file topic folder and select **New**.

The New File Signature dialog appears:



3. Select the Search Expression tab (the default display) and enter the search expression in the Search Expression field.
4. Give the file signature a descriptive name.
5. Select **Case Sensitive** if appropriate.

6. Click the Extensions tab and enter the file's three-letter extension. You can enter more than one file extension by separating them with a semicolon.



7. Add the suffix `_*` to the file extension to include it in Vista Shadow Directories. It looks like this: `<extension>_*`
8. Click **OK**.

The file signature is added to the table.

## Editing a Signature

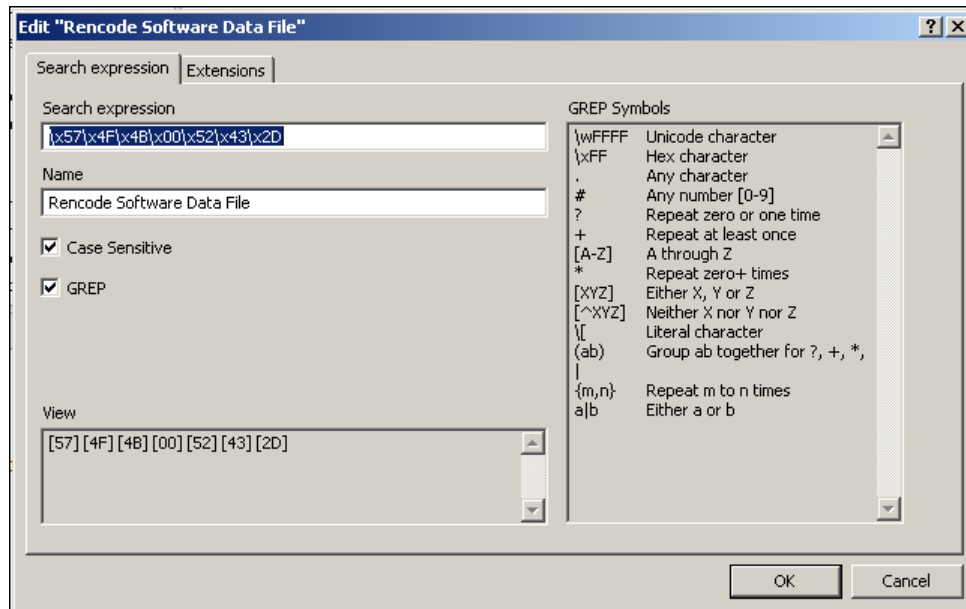
Use this procedure to edit an existing file signature.

1. Click **View > File Signatures**.

The file signature category list appears in the Tree pane. When you select a category, its signature contents appear in the Table pane.

2. Right-click a signature from the Table pane and select **Edit**.

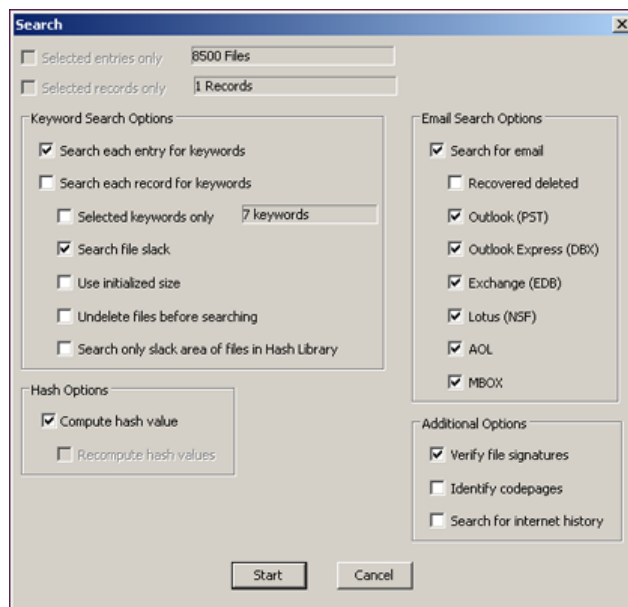
An Edit selected signature name dialog appears.



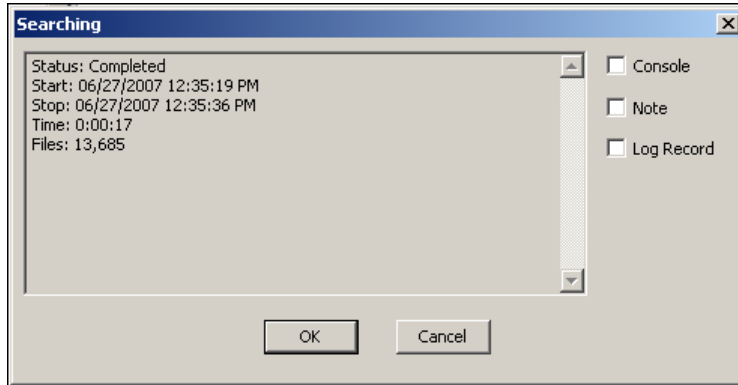
3. Change the **Search Expression** and other fields as desired, and click **OK**.

## Performing a Signature Analysis

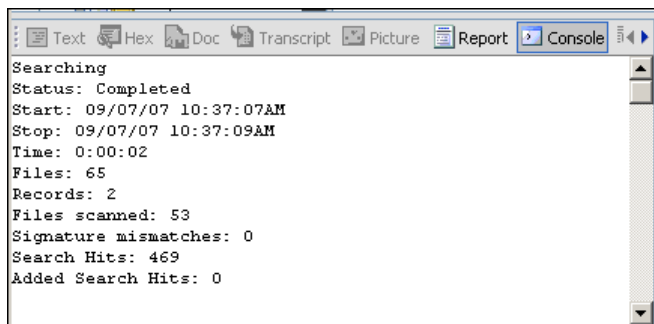
To begin a signature analysis, click **Search**.



Check the **Verify file signatures** box in the **Additional Options** area in the lower right, then click **Start**. The signature analysis routine runs in the background. On completion, a search complete dialog appears. The dialog presents search status, times, and file data.

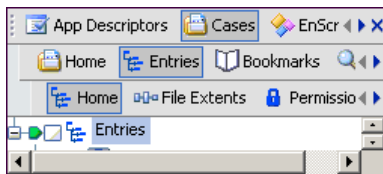


You can view these same data in the console.



## Viewing Signature Analysis Results (Part 1)

Click **Set-Include** in the Tree pane to display all files in the case.



At this level, Set Include selects everything in the evidence file.

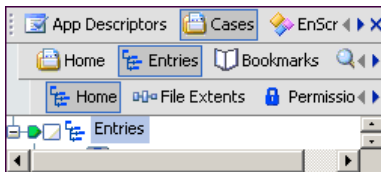
1. Organize the columns in the Table pane so that the Name, File Ext, and Signature columns are next to each other.
2. Sort columns with Signature at first level, File Ext at second level and Name at third level.

Scroll up or down to see all the signatures.

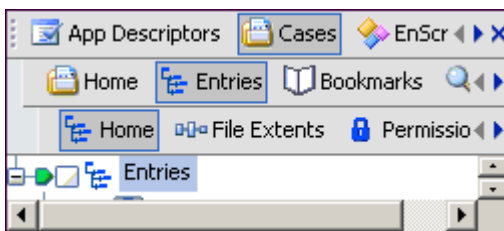
	Name	Signature	File Ext	File Type
410	9387129_120_1[1].gif	* AOL ART	gif	GIF
411	9388114_120_1[1].gif	* AOL ART	gif	GIF
412	9415634_120_1[1].gif	* AOL ART	gif	GIF
413	AAAAAAXGPJ[1].GIF	* AOL ART	GIF	GIF
414	AAAAAAZDGZ[1].GIF	* AOL ART	GIF	GIF
415	account_icon[1].gif	* AOL ART	gif	GIF
416	address_icon[2].gif	* AOL ART	gif	GIF
417	aim[1].gif	* AOL ART	gif	GIF
418	all_off[1].gif	* AOL ART	gif	GIF
419	all_on[1].gif	* AOL ART	gif	GIF
420	alternate_728x90_15k[1].gif	* AOL ART	gif	GIF
421	aolhometown[1].gif	* AOL ART	gif	GIF
422	auction_icon[1].gif	* AOL ART	gif	GIF
423	bcwipe_ss[1].gif	* AOL ART	gif	GIF
424	block_carley_ZDNet[1].gif	* AOL ART	gif	GIF

## Viewing Signature Analysis Results (Part 2)

1. Click **Set-Include** in the **Entries** selection in the Tree pane.



A list of case files and their associated file signature and other data appears in the Table pane.



2. Sort the data if desired. In this case, the red triangle in the **Name** column indicates the display is sorted alphabetically by name.

## Signature Analysis Legend

Signature analysis identifies and organizes file signatures with reference to what it finds in:

- the signature table
- the file header, and
- extension as they appear in the evidence file.

**Match** in the Legend column indicates data in the file header, extension and File Signature table all match.

**Alias** means the header is in the File Signature table but the file extension is incorrect, for example, a JPG file with a .ttf extension.

This indicates a file with a renamed extension. The name in the Legend column below (next to the asterisk) displays the type of file identified by the file signature.

---

Note: An alias is preceded by an asterisk, such as \*AOL ART.

---

**Unknown** means neither the header nor the file extension is in the File Signature table.

**!Bad Signature** means the file's extension has a header signature listed in the File Signature table, but the file header found in the case does not match the File Signature table for that extension.

The table shows possible results of a signature analysis.

Signature Analysis Table			
File Name	Signature Table	Header Entry	Legend
ball.jpg	FF D8 FF E1	ÿøÿá	Match
leftshop.gif	4A 47 04 0E	JG . .	*AOL ART {Alias}
flagfile.ph	5B 77 6D 71	[wmq]	Unknown
userinfo.bag	41 4F 4C 20	AOL .	!Bad Signature

## EnScript Programming Language

The EnScript® language is a programming language and Application Program Interface (API) designed to operate within the EnCase software environment. Although similar in many ways to C++ and Java, not all their functions are available in the EnScript language. Classes, and their included functions and variables, are found in the EnScript Types tab in the Tree pane.

---

Note: The EnScript language uses the same operators and general syntax as C++, though classes and functions are different.

---

Our message board at <https://messageboards.guidancesoftware.com/forumdisplay.php?f=11> (<https://messageboards.guidancesoftware.com/forumdisplay.php?f=11>) provides additional information about the EnScript language.

## Included Enscript Components

EnCase® software comes bundled with a number of EnScript programs.

The EnCase installer puts these programs in the default EnCase folder. Its address is typically C:\Program Files\EnCase\EnScript. This folder in turn contains four subfolders visible by clicking EnScript in the **Filters** pane. They are

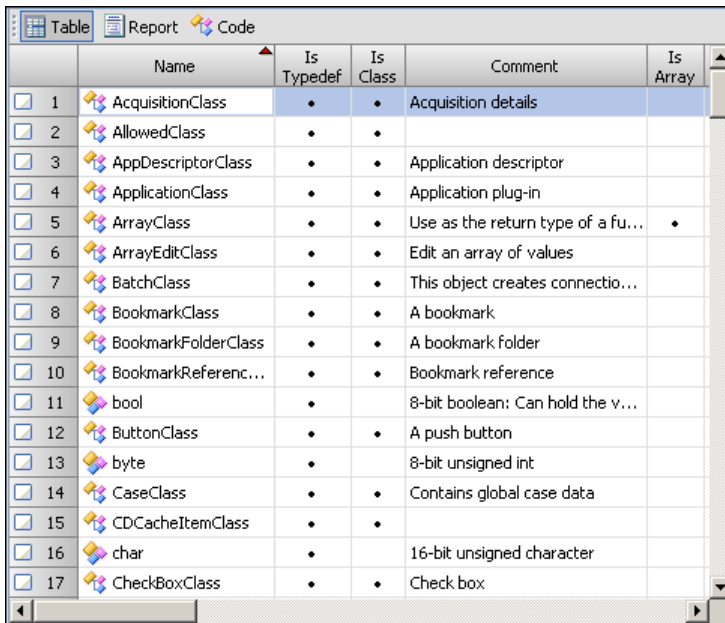
- Examples
- Forensic
- Include
- Main

Enterprise users have an additional Enterprise folder. Each folder contains the include directory and libraries.

## EnScript Types

EnScript **types** reference resources in EnScript language classes. Perusing these provides information about EnCase classes and functions.

To view EnScript Types, click **View > EnScript Types**.



	Name	Is Typedef	Is Class	Comment	Is Array
<input checked="" type="checkbox"/> 1	AcquisitionClass	•	•	Acquisition details	
<input checked="" type="checkbox"/> 2	AllowedClass	•	•		
<input checked="" type="checkbox"/> 3	AppDescriptorClass	•	•	Application descriptor	
<input checked="" type="checkbox"/> 4	ApplicationClass	•	•	Application plug-in	
<input checked="" type="checkbox"/> 5	ArrayClass	•	•	Use as the return type of a fu...	•
<input checked="" type="checkbox"/> 6	ArrayEditClass	•	•	Edit an array of values	
<input checked="" type="checkbox"/> 7	BatchClass	•	•	This object creates connectio...	
<input checked="" type="checkbox"/> 8	BookmarkClass	•	•	A bookmark	
<input checked="" type="checkbox"/> 9	BookmarkFolderClass	•	•	A bookmark folder	
<input checked="" type="checkbox"/> 10	BookmarkReferenc...	•	•	Bookmark reference	
<input checked="" type="checkbox"/> 11	bool	•		8-bit boolean: Can hold the v...	
<input checked="" type="checkbox"/> 12	ButtonClass	•	•	A push button	
<input checked="" type="checkbox"/> 13	byte	•		8-bit unsigned int	
<input checked="" type="checkbox"/> 14	CaseClass	•	•	Contains global case data	
<input checked="" type="checkbox"/> 15	CDCacheItemClass	•	•		
<input checked="" type="checkbox"/> 16	char	•		16-bit unsigned character	
<input checked="" type="checkbox"/> 17	CheckBoxClass	•	•	Check box	

The Tree pane contains a list of classes. Double-clicking an entry provides additional detail for the class.

## Hash Analysis

A hash function is a way of creating a digital fingerprint from data. The function substitutes or transposes data to create a hash value. Hash analysis compares case file hash values with known, stored hash values.

The hash value is commonly represented as a string of random-looking binary data written in hexadecimal notation. If a hash value is calculated for a piece of data, and one bit of that data changes, a hash function with strong mixing property usually produces a completely different hash value.

A fundamental property of all hash functions is that if two hashes (according to the same function) are different, then the two inputs are different in some way. On the other hand, matching hash values strongly suggests the equality of the two inputs.



## File Hashing

Hashing creates a digital fingerprint of a file. This fingerprint is used to identify files whose contents are known to be of no interest, such as operating system files and the more common application.

EnCase uses an MD5 hashing algorithm, and that value is stored in the evidence files. The MD5 algorithm uses a 128-bit value. This raises the possibility of two files having the same value to one in  $3.40282 \times 10^{38}$ .

Any mounted drive, partition, or file can be hashed. The hash value produced can be validated and used in the program. By building a library of hash values, the application checks for the presence of data with a hash value contained in the hash library. The hash value is determined by the file's contents. It is independent of the file's name, so the file's hash value is calculated by the program and identified as matching a value in the hash library, even if the file's name has changed.

## Hash a New Case

When a case is initially created, it is not hashed. Before comparing the case's data with a library of known or notable files, hash the case. The Table pane display may look like this:

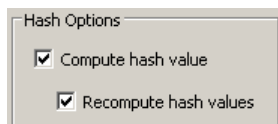
	Name	Hash Value
<input type="checkbox"/> 4	HashSearchScreen....	
<input type="checkbox"/> 5	buttonSearch.bmp	
<input type="checkbox"/> 6	HashFinished Searc...	
<input type="checkbox"/> 7	_PPDES~3.PNG	
<input type="checkbox"/> 8	app descriptor utilit...	
<input type="checkbox"/> 9	_MP2D6.TMP	
<input type="checkbox"/> 10	app descriptor scan...	
<input type="checkbox"/> 11	app descriptor scan...	

Open a case that needs hashing and display its contents.








1. Click the Search tab.

The Search dialog appears.

2. Make any search choices and then select the required values in the Hash Options area of the dialog.
3. Click **Start**.



The Table pane contents changes and shows the newly created hash values for the files.

	Name	Hash Value
<input checked="" type="checkbox"/> 2	 FurBall.BMP	d01b79c3aafe3462297a2ae8b57c87b1
<input checked="" type="checkbox"/> 3	 Table View.BMP	e86c121180451b6b23871eaae88c871c
<input checked="" type="checkbox"/> 4	 HashSearchScreen....	ea437730f85f08c8456172b56c891e3
<input checked="" type="checkbox"/> 5	 buttonSearch.bmp	f1b2186d8feac94b9b64d245c987c741
<input checked="" type="checkbox"/> 6	 HashFinished Searc...	06afb63e5039043f0168e85fb4d25037
<input checked="" type="checkbox"/> 7	 _PPDES~3.PNG	
<input checked="" type="checkbox"/> 8	 app descriptor utilit...	

## Hash Sets

Hash sets are collections of hash values (representing unique files) that belong to the same group. For example, a hash set of all Windows operating system files could be created and named Windows System Files. When a hash analysis is run on an evidence file, the software identifies all files included in that hash set. Those logical files can then be excluded from later searches and examinations. This speeds up keyword searches and other analysis functions.

### Create a Hash Set

Analyzing files by identifying and matching the unique MD5 hash value of each file is an important part of the computer forensics process. The hash library feature allows the investigator to import or custom build a library of hash sets, enabling the expedient identification of any file matches in the examined evidence.

Computer forensics analysts often create different hash sets of known illegal or unapproved images, hacker tools, or non-compliant software to quickly isolate any files in an investigation that are included in that set.

Hash sets, once created, are kept indefinitely and added to on a case by case basis. Adding new files as time goes by saves time and effort in subsequent investigations.

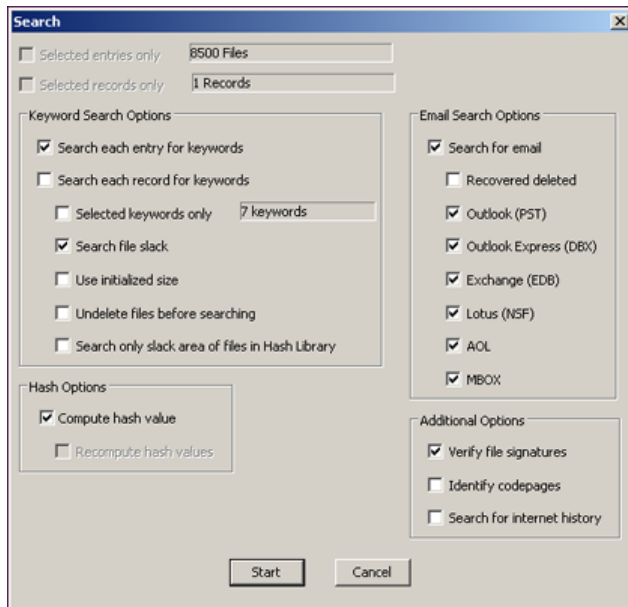
---

**Note:** When creating hash sets to identify suspect software (such as non-licensed software, steganography or counterfeiting utilities), it is important that the investigator carefully construct sets to prevent false positives.

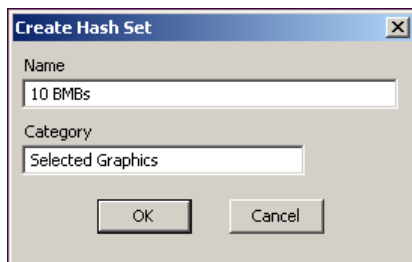
---

1. Open the case and click **Search**.

The search dialog appears.



2. In the Hash Options area, check **Compute Hash Values**.
3. Select files to be included in the hash set.
4. Right-click the Table pane and select **Create Hash Set** from the menu. The Create Hash Set dialog appears.



5. Enter a set Name and Category, and click **OK**.

A hash set is created.

---

Note: While the Category entry can be anything, the two industry standards are **Known** and **Notable**, with the latter being assigned hash values that are of interest to the investigator.

---

## Rebuild a Hash Library

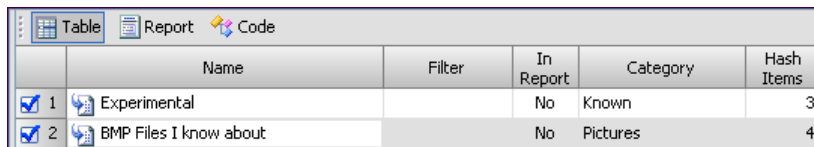
To select a hash set to used in a case, rebuild the library.

---

**Note:** Only items selected on the Hash Sets tab are included in the library.

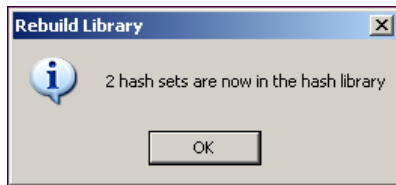
---

1. Select **View > Hash Sets**. A list of hash sets appears.



	Name	Filter	In Report	Category	Hash Items
<input checked="" type="checkbox"/> 1	Experimental		No	Known	3
<input checked="" type="checkbox"/> 2	BMP Files I know about		No	Pictures	4

2. Select the desired hash set.
3. Right-click and select **Rebuild Library** from the menu. When Rebuild completes, a message indicating the number of rebuilt libraries appears.



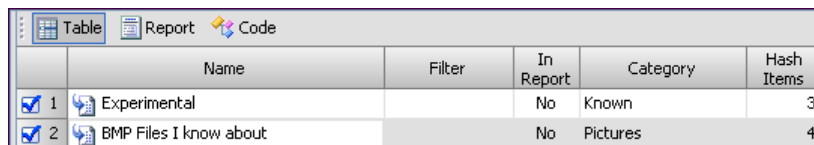
## Viewing Hash Search Results

When files in a case are hashed, they are compared to the library, then the hash set and hash category columns populate.

After rebuilding your library and hashing the case files, view the results in the Table pane.

1. Select **View > Hash Sets** from the main menu.

A list of all hash sets appears in the Table pane.



	Name	Filter	In Report	Category	Hash Items
<input checked="" type="checkbox"/> 1	Experimental		No	Known	3
<input checked="" type="checkbox"/> 2	BMP Files I know about		No	Pictures	4

If a file with the same hash value is contained in the hash library, its columns are populated.

## Keyword Searches

EnCase applications provide a powerful search engine to locate information anywhere on physical and logical media in a current, open case. Global keywords can be used in any case, or they can be made case-specific and used only within the existing case.

A *keyword* in a search is an expression used to find words within a case that match the keyword entries. The EnCase search engine accepts a number of options, and is particularly powerful searching regular expressions with a GREGP- formatted keyword.

---

Note: In addition to GREGP, the search can be limited by making it case sensitive and selecting particular codepages. Codepages are alphabet sets of a variety of Latin and non-Latin character sets such as Arabic, Cyrillic, and Thai.

---

The keywords included in the software give an investigator the ability to search

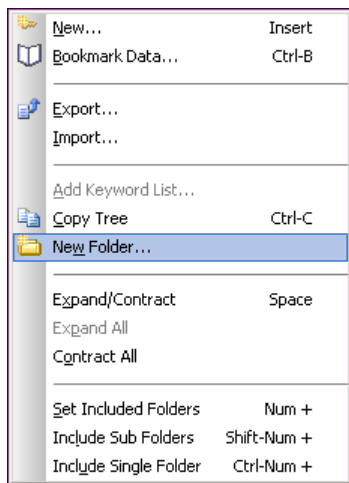
- Email addresses
- Web addresses
- IP addresses
- Credit card numbers
- Phone numbers
- Dates with a four-digit year

## Creating Global Keywords

Global keyword lists should be analyzed and targeted, then assigned to discrete folders. These folders are accessible by any case.

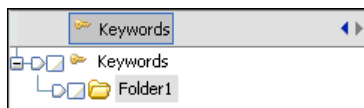
1. Click **Keywords** from the Tree pane.

This menu appears:



2. Right-click the Keywords icon in the Tree pane, and click **New Folder**.

The Tree pane of the keywords tab changes showing an additional folder.



3. Rename the folder as desired.

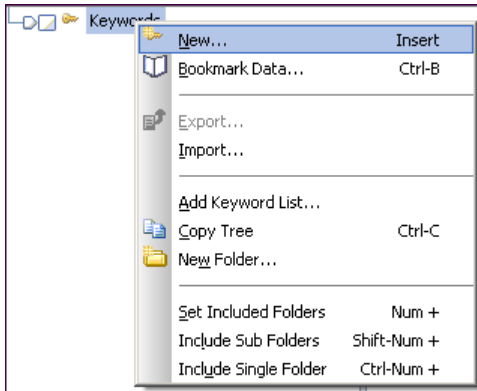
## Adding Keywords

Add keywords directly to a new folder, an existing folder, or the root folder.

Open the Tree pane from the Keywords tab.

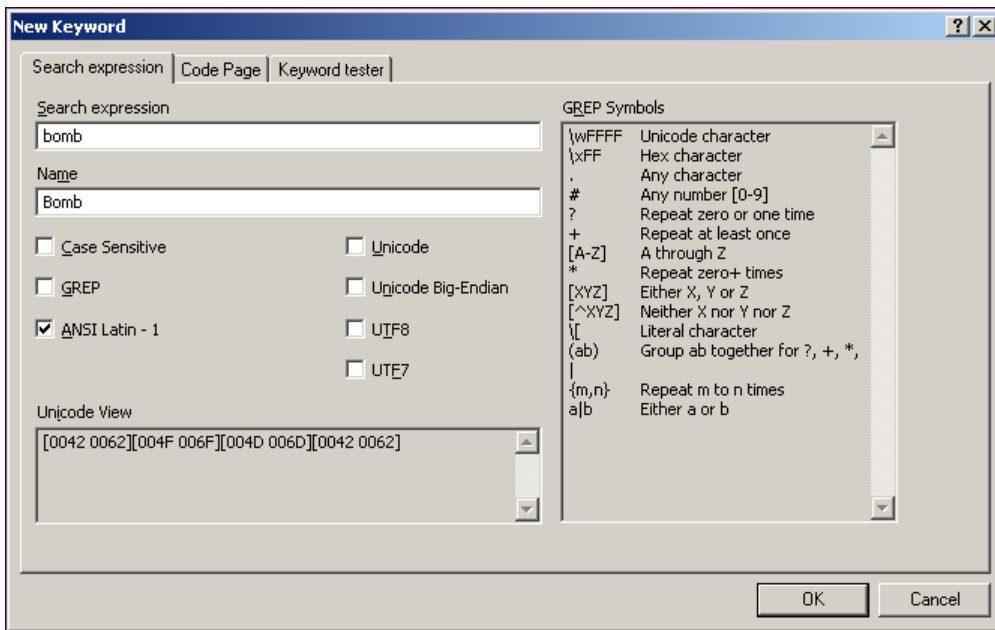
1. Right-click a keyword entry in the Tree pane.

This menu appears if the main Keywords icon is selected. If a sub-folder is selected, the menu is slightly different in appearance, but functions the same.



2. Click **New**.

The New Keyword Dialog appears.



3. Complete the dialog as described here:

**Search Expression** is the actual text being searched.

**Name** is the search expression name listed in the folder. **Case Sensitive** searches the keyword only in the exact case specified.

**GREP** uses GREP syntax for the search.

---

Note: Previously the ANSI Latin - 1 option was called Active Code Page. Since the Active Code Page varied according to the Active Code Page running on the Examiner machine at the time, it was replaced by ANSI Latin - 1 to insure consistent search results.

---

**ANSI Latin - 1** is the default code page. It searches documents using the ANSI Latin - 1 code page.

**Unicode:** select if you are searching a Unicode encoded file. Unicode uses 16 bits to represent each character. Unicode on Intel-based PCs is referred to as **Little Endian**. The Unicode option searches the keywords that appear in Unicode format only. For more details on Unicode, see <http://www.unicode.org>.

---

Note: The Unicode standard attempts to provide a unique encoding number for every character, regardless of platform, computer program, or language.

---

**Big-Endian Unicode:** select if you are investigating a Big-Endian Unicode operating system (such as a Motorola-based Macintosh). Big-Endian Unicode uses the non-Intel data formatting scheme. Big-Endian operating systems address data by the most significant numbers first.

**UTF-8** meets the requirements of byte-oriented and ASCII-based systems. UTF-8 is defined by the Unicode Standard. Each character is represented in UTF-8 as a sequence of up to four bytes, where the first byte indicates the number of bytes to follow in a multi-byte sequence.

---

Note: UTF-8 is commonly used in Internet and Web transmission.

---

**UTF-7** encodes the full BMP repertoire using only octets with the high-order bit clear (7 bit US-ASCII values, [US-ASCII]). It is deemed a mail-safe encoding.

---

Note: UTF-7 is mostly obsolete, and is used when searching older Internet content.

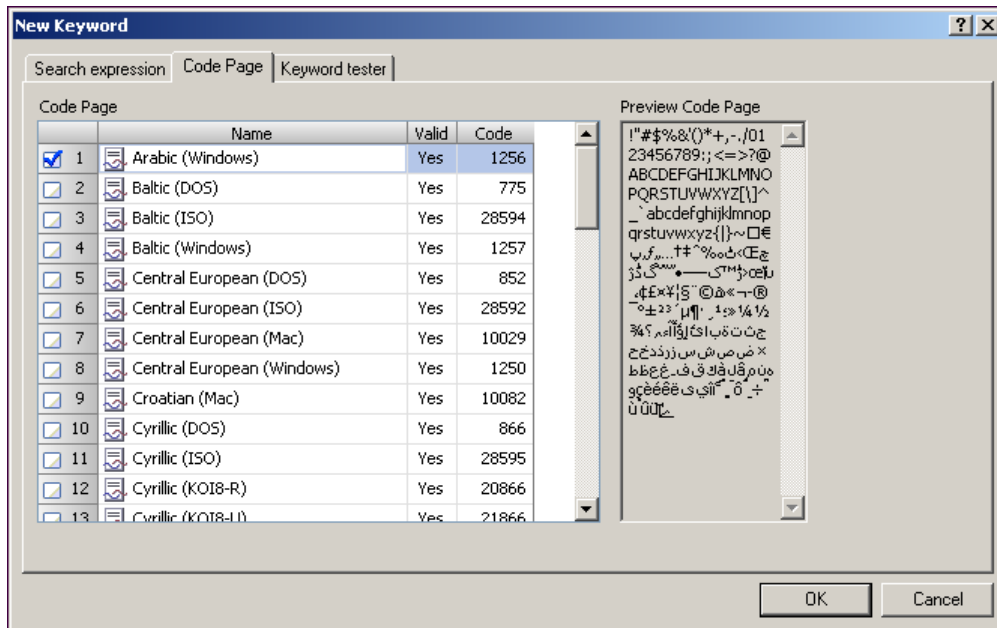
---



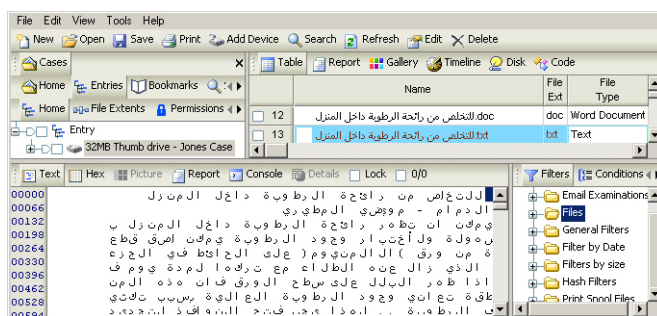
## Creating International Keywords

You can search international keywords of non-English character sets. This allows an investigator to enter, search, and locate words written in Japanese, Arabic, or Russian, for example. Keyword hits and the document display in the original language.

1. Select the Code Page tab on the New Keyword dialog. A list of supported language sets appears. Here, the Arabic Code Page is checked:



2. Return to the Search Expression tab of the dialog and enter the keyword. Perform a search as usual.



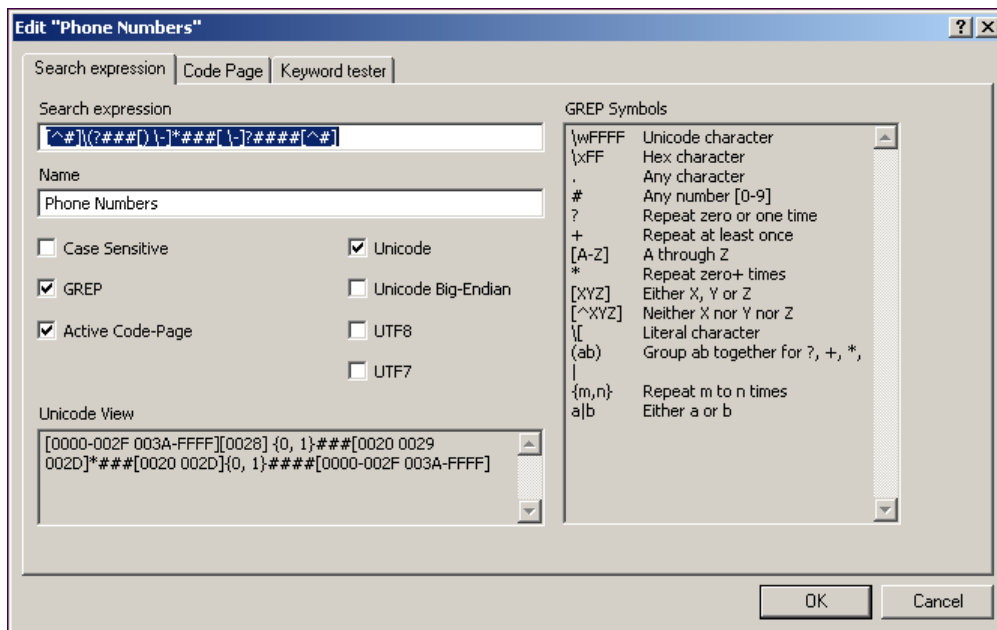
Results appear as in a usual keyword search.

## Keyword Tester

To test a search string against a known file, click the **Keyword Tester** tab. Enter an expression in the Search Expression field and be sure to select the proper keyword options.

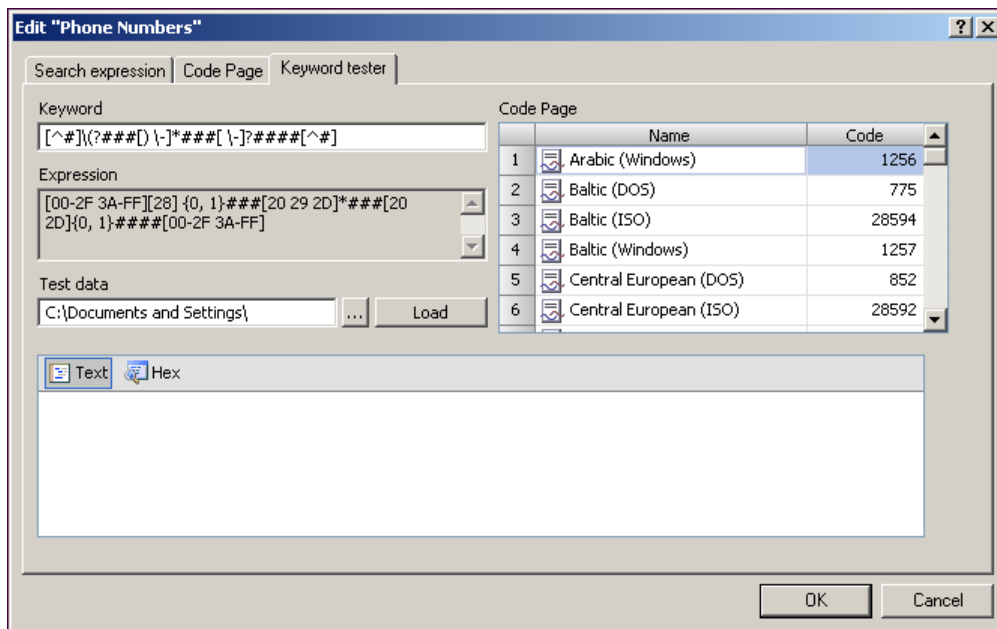
1. Add a new keyword (see *Adding Keywords* (on page 344)).
2. Add an expression and name the keyword.

In this case, a GREP keyword designed to capture telephone numbers is entered:



3. Select the desired options (for example, Case Sensitive or GREP).

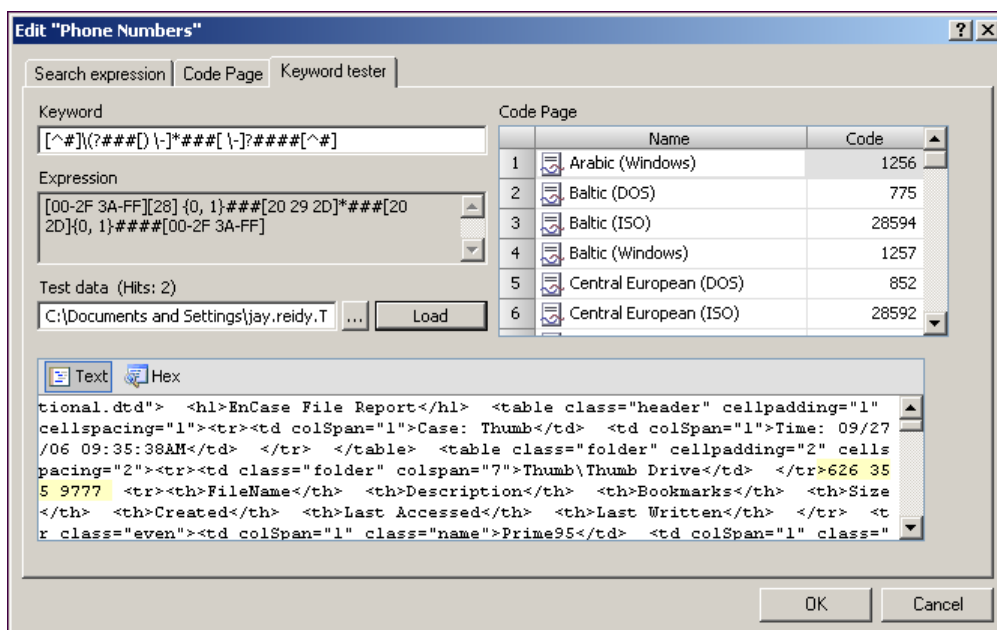
4. Select the Keyword Tester tab.



5. Locate a test file that contains the search string, enter the address into the Test Data field, and click **Load**.

The test file is searched and displays in the lower tab of the Keyword Tester form.

Note: Hits are highlighted in both text view and hex view.



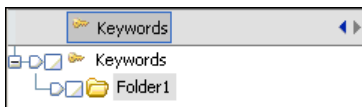
## Local Keywords

A local keyword is associated with a unique case, and can be searched for only when that case is open. If a local keyword is created in one case, and another is opened, the local keyword is unavailable.

Open a case and prepare a list of keywords specific to this case only.

1. Select **View>Cases Sub-Tabs> Keywords**.

The Tree pane appears with a display something like this. This specific display shows the local keywords folder with a new folder added.



## Import Keywords

You can import keywords and keyword lists from other users. To import a keyword list:

1. Right-click a keyword folder in the Tree pane.
2. Select **Import**.
3. Enter or browse to the path of the desired file and click **OK**.

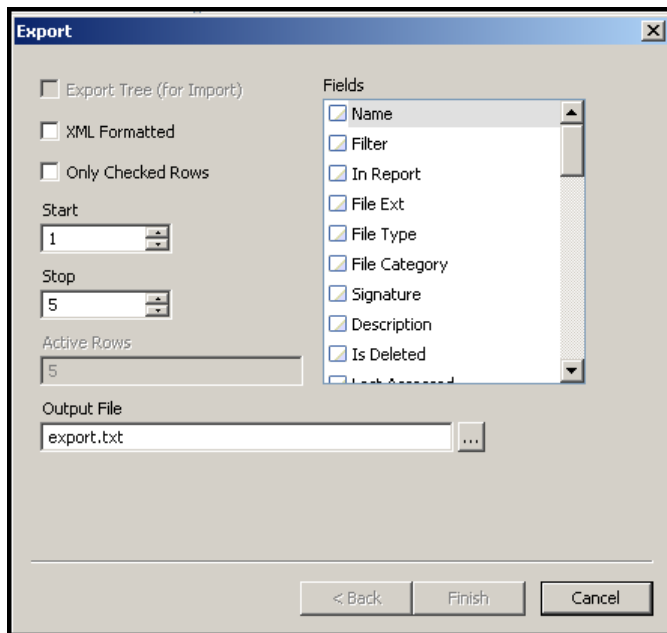
The imported list appears in the Tree pane.

## Export Keywords

Keywords are exported in .txt file format. You can export all keywords at one time or create a list of selected keywords for transfer.

1. Right-click a keyword in the Table pane.
2. Select **Export**.

Complete the dialog.



3. Check **Export Tree (for Import)** and click **OK**.

---

**Note:** To export a .txt file into Excel, do not select **Export Tree**.

---

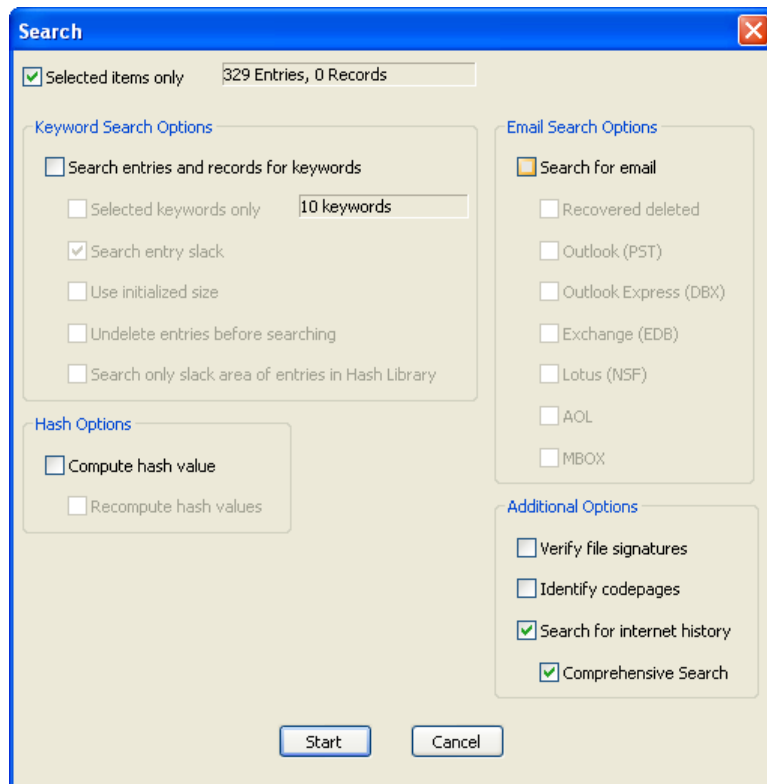
Check **XML Formatted** to export table rows or the tree structure to an XML formatted file.

## Searching Entries for Email and Internet Artifacts

Records are created when email or Internet history searches are performed.

EnCase searching can parse areas outside of logical file content (unallocated clusters and volume slack) for Internet History and add this data to the Records tab for further investigation.

The Search dialog box features a new checkbox, *Comprehensive search*, to support this feature. When you select Search for Internet history, the Comprehensive Search box is enabled.



---

Note: Selecting Comprehensive Search increases the time it takes to complete the search.

---

*To create a record :*

1. Click **Search**.  
A search dialog appears.
2. Select options and click **Start**.
3. Select **Search for Internet History** and **Comprehensive Search** to search for Internet history (including searching file slack and unallocated space).
4. When the search finishes, click **View > Cases Sub-Tabs > Records**.

Finding history and cache results may require moving down the tree several levels.

Newly created records display in the Table pane. The Tree pane shows the type of record and the Table pane shows the files within that record. If there are additional details regarding a file selected in the Table pane, click **Additional Fields** in the Tree pane to see that information.

The screenshot displays the EnCase Enterprise Training application interface. The top menu bar includes File, Edit, View, Tools, and Help. Below the menu is a toolbar with icons for New, Open, Save, Print, Add Device, Search, Logon, and Refresh. The main interface is divided into several panes:

- Tree Pane (Left):** Shows a hierarchical view of the case. The 'Records' folder is expanded, showing 'Hunter XP' and 'C'. Under 'C', 'Internet Explorer (Windows)' is expanded, showing 'History' and 'Cache'.
- Table Pane (Middle):** Displays a list of files found within the selected record. The table has columns for Name, Filter, In Report, Search Hits, Additional Fields, Message Size, and Creation Time. The files listed include:
 

Name	Filter	In Report	Search Hits	Additional Fields	Message Size	Creation Time
1 wuv3s[1].tgz			•	•	88211	03/31/02 06:16:46AM
2 index.dat			•	•	104	03/31/02 06:16:29AM
3 index.dat			•	•	104	03/31/02 06:16:27AM
4 adsWrapper[1].js			•	•	6266	06/04/02 05:15:23PM
5 arrow_y[1].gif			•	•	108	06/04/02 05:19:13PM
6 adsEnd[1].js			•	•	33	06/04/02 05:15:26PM
7 index.dat			•	•	138	
8 usedlets[1].gif			•	•	915	05/14/02 10:00:16AM
9 usvomenctr[1].gif			•	•	763	05/14/02 10:00:16AM
10 expedat[1].gif			•	•	871	05/14/02 10:00:16AM
11 pan_swest_on_south[1].gif			•	•	89	06/04/02 05:35:39PM
12 hotmail_7[3].css			•	•	4932	03/31/02 06:34:15AM
13 btn_zoomnotch[2].gif			•	•	60	06/04/02 05:35:40PM
14 icon_maps_large[1].gif			•	•	1707	06/04/02 05:35:05PM
15 Grey_Rebuild[1].gif			•	•	9768	06/04/02 05:41:31PM
16 login_mid_line[1].nif			•	•	943	03/31/02 07:26:04AM
- Main Pane (Bottom):** Displays a hex view of the selected file, 'wuv3s[1].tgz'. The hex data is shown in columns, with the corresponding ASCII characters displayed to the right. The data appears to be a compressed file format, likely a tar.gz archive.
- EnScript Pane (Right):** Shows a list of EnScript scripts, including 'Enterprise', 'Examples', 'Forensic', 'Include', and 'Main'.

The status bar at the bottom indicates the current case: 'V5 Test Case\Hunter XP\C\WINDOWS\system32\config\systemprofile\Local Settings\Temporary Internet Files\Content.IE5\WFK38883\wuv3s[1].tgz (PS 898387 LS 898324 CL 224581 SO 000 FO 0 LE 88211)'.

Common columns in the Report pane are:

**Name** is the file name and extension.

**Filter** shows if a filter was applied.

**In Report** is a True or False indicator of files present in a report. To change the selection, enter **CTRL + R**.

**Search Hits** indicates whether the file contains a keyword search word.

**Additional Fields:** when True, indicates that additional fields were found in the record. Data contained in the Additional fields varies depending on the type of data in the record.

**Message Size:** the message size in bytes.

**Creation Time** is the date and time the message was created in mm/dd/yy hh:mm:ss format. AM or PM is attached as appropriate.

**Profile Name** is the owner of the message.

**URL Name** is the name of the URL where the message originated.

**URL Host** is the name of the URL host where the message originated.

**Browser Cache Type** shows the format in which cached data are stored. Options include image, code, HTML, and XML.

**Browser Type** is the browser where the artifact was viewed, such as Internet Explorer or Firefox.

**Last Modification Time** is the last time the cache entry was updated.

**Message Codepage** is the code page type for reading this cache entry.

**Last Access Time** shows the last time the cache entry was retrieved or loaded.

**Expiration** is the time when this cache becomes stale and is deleted from the cache.

**Visit Count** is number of times this cache entry was accessed by the browser.

**Server Modified** is the last time the cached item was modified on the server where it was cached.



## Internet History Searching

Currently, five browsers and two types of Internet history are supported. They are:

- Internet Explorer, history and cache
- Macintosh Internet Explorer, history and cache
- Safari, history and cache
- Firefox, history and cache
- Opera, history and cache

---

Note: The difference between a regular search and a search of unallocated is that keywords are added internally and marked with a special tag indicating it is for Internet history searching only.

---

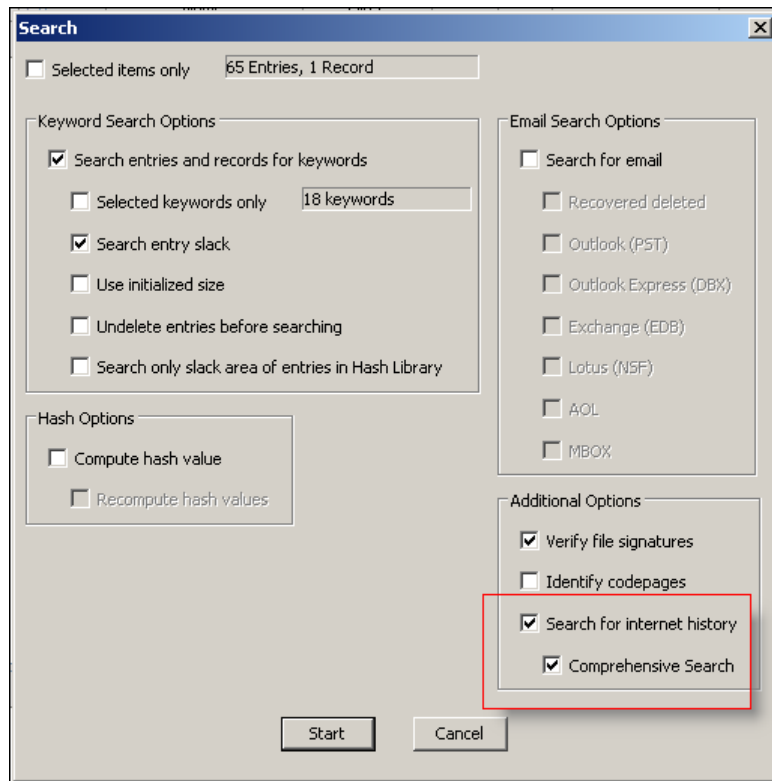
## Comprehensive Internet History Search

A **comprehensive Internet history search** differs from a regular Internet search. Specially tagged keywords are added internally and the software takes a different code path than a regular search. In this comprehensive search, EnCase examines the entire device (including file slack and unallocated space) for specific markers that indicate Internet artifacts. The basic Internet history search parses known file types for Internet artifacts.

The latest version of EnCase® software and either Windows XP or 2000 must be installed. Begin an unallocated space search the same way you begin a regular search.

1. Select **Comprehensive Search** in the Search Dialog.

Selecting **Search for Internet History** at the same time, as shown in the figure, performs a regular Internet history search in addition to the exhaustive search.



These fields are added to the **Browser Cache Type** field:

- Audio
- Video
- XML
- Text

## Internet Searching

The search engine can search evidence files for various Web artifact types. The Internet search feature can search Internet Explorer, Mozilla Firefox, Opera, and Safari.

Use the search dialog for Internet searching. Results are viewed on the Records tab. For information on that procedure, see Searching Entries For Email and Internet Artifacts and Viewing Record Search Hits.

## Performing a Search

You can search an entire case, an entire device, or an individual file or folder. For example, when searching information in unallocated space, such as a file header, select the Unallocated Clusters to avoid having to search the entire case.

1. Click the Search button on the tool bar. The Search form appears.
2. Complete the dialog and click **Start**.

See *Search Options* (on page 357) for help completing the search dialog.

## Search Options

You can use a number of options to customize a search.

The screenshot shows the 'Search' dialog box with the following options:

- ☒ Selected items only: 329 Entries, 0 Records
- Keyword Search Options**
  - ☐ Search entries and records for keywords
    - ☐ Selected keywords only: 10 keywords
  - ☒ Search entry slack
  - ☐ Use initialized size
  - ☐ Undelete entries before searching
  - ☐ Search only slack area of entries in Hash Library
- Hash Options**
  - ☐ Compute hash value
    - ☐ Recompute hash values
- Email Search Options**
  - ☒ Search for email
    - ☐ Recovered deleted
    - ☐ Outlook (PST)
    - ☐ Outlook Express (DBX)
    - ☐ Exchange (EDB)
    - ☐ Lotus (NSF)
    - ☐ AOL
    - ☐ MBOX
- Additional Options**
  - ☐ Verify file signatures
  - ☐ Identify codepages
  - ☒ Search for internet history
  - ☒ Comprehensive Search

Buttons: Start, Cancel

**Selected items only** runs a search for items limited to the files, folders, records, or devices that you checked.

**Search entries and records for keywords:** executes a keyword search when checked. When unchecked, other checked functions are performed, but the keyword search is not. This allows you to run a signature analysis or a hash analysis without running a keyword search. This option also enables:

- Selected keywords only
- Search entry slack
- Use initialized size
- Undelete entries before searching
- Search only slack area of entries in Hash Library

**Selected keywords only** restricts the number of keywords used during the keyword search to the number of keywords specified (shown in **Number of Keywords**).

**Search entry slack** searches the slack area between the end of logical files and the end of their respective physical files.

**Use initialized size** searches only the initialized size of an entry (as opposed to the logical or physical size).

---

Note: Initialized size is only pertinent to NTFS file systems; when a file is opened, if the initialized size is smaller than the logical size, the space after the initialized size is zeroed out. Thus, searching the initialized size searches only data a user would see in a file.

---

**Undelete entries before searching** undeletes deleted files prior to searching.

**Search only slack area of entries in Hash Library** is used in conjunction with a hash analysis.

**Verify file signatures** performs a signature analysis during a search.

**Compute hash value** performs a hash analysis during a search.

**Recompute hash value** regenerates previously computed hash values.

**Search for Email** turns on dialog email search options.

**Recover Deleted** accesses deleted email.

**Email Type List** provides options for email that can be recovered.

**Verify Signatures** performs a signature analysis during a search. It determines whether the file extension matches the signature assigned to that file type.

**Identify Codepages** tries to detect the code page for a file.

**Search for Internet History** recovers Web data cached in the Web history file.

**Comprehensive Search** searches for Internet history in unallocated space.

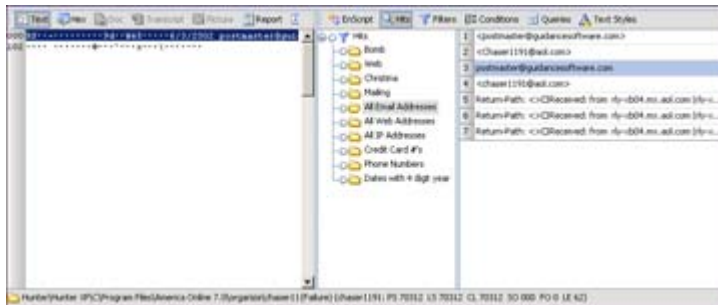
## Viewing Record Search Hits

Records are virtual files created when email or Internet history searches are performed.

Searching records is straightforward.

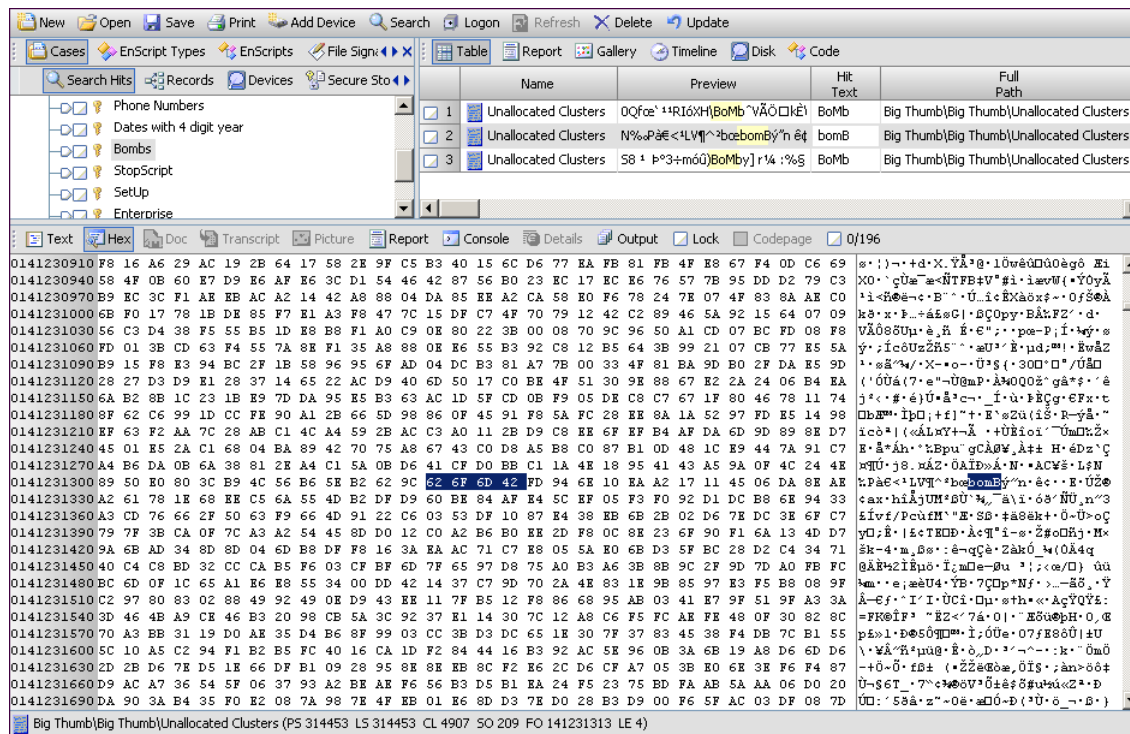
1. Click **Records** when the search finishes.
2. Select **Set-Include**.
3. Select a record that shows a search hit.
4. Select **Hits** on the Filter pane.
5. Click keyword folders one by one to see search hits.

The newly created records are now visible.



## Viewing Search Hits

Search hits are organized by each keyword appearing in the Tree pane. Search hits within each keyword appear in the Table pane.



To view your search hits:

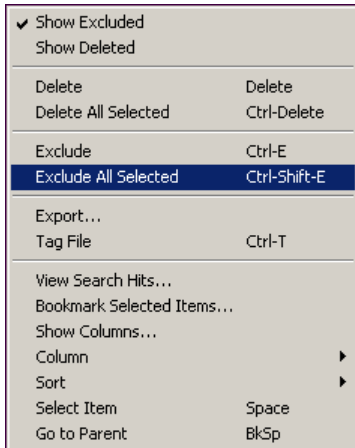
- Click the **Search Hits** tab in the menu bar or
- Click **View > Cases Sub- Tabs Search Hits**

## Exclude Files

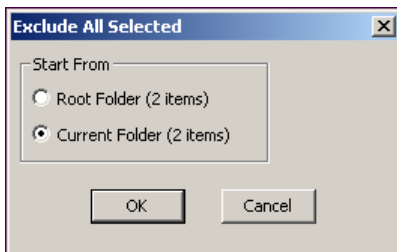
Sometimes a keyword search returns more files than are useful to report. Hide these files from view by excluding them.

Run, then view a keyword search.

1. Select files to exclude, then right-click the view.
2. Select either **Exclude** or **Exclude All Selected**.



Selecting **Exclude All Selected** displays a second option dialog.



3. Select the appropriate option and click **OK**.

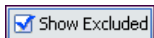
The selected files disappear from view.

## Show Excluded Files

Excluded files are not deleted. They are merely hidden from view. To see them again, select the Show Excluded function.

To show excluded files:

1. Select **Show Excluded**.



Excluded files reappear in Table and Report view.

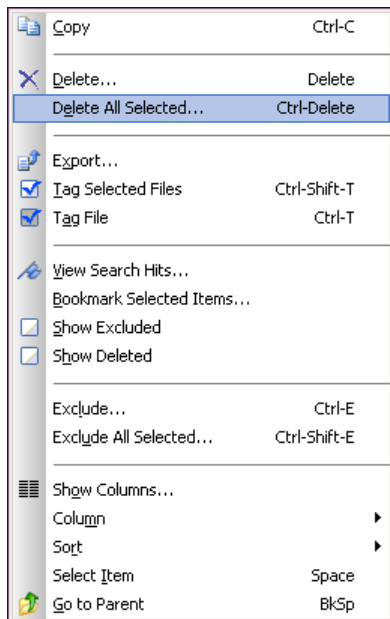
## Deleting Items

When using Search Hits, delete is considered a soft delete which you can undelete until the case is closed. If a search hit remains deleted when the case is closed, the hit is permanently deleted. In other tabs, however, undelete works only with the last selection deleted. Once a file is closed, deleted items are permanently removed and cannot be recovered.

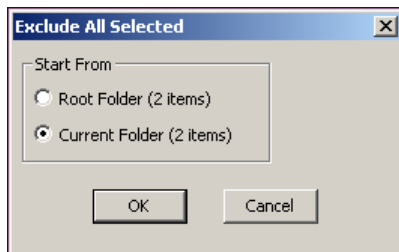
Run, then view a keyword search. This process is similar to *Exclude Files* (on page 360).

View the search hits report in the Table pane before excluding them from the report.

1. Select files to exclude, then right-click the view.
2. Select either **Delete** or **Delete All Selected**.



Selecting the latter displays the **Exclude All Selected** dialog.



3. Select the appropriate option and click **OK**.

The selected files are temporarily deleted.

---

**Note:** Viewing the report shows the concatenated results.

---



## Show Deleted Files

Excluded files are not deleted. They are merely hidden from view. To see them again, select the Show Excluded function.

---

Note: Deleted files are stored in a temporary buffer until the file is closed, at which time the buffer and deleted files are erased.

---

Exclude a number of files.

To review excluded files:

1. Click **Show Excluded**.

Deleted files reappear in both Table pane and in Report pane.

## Encode Preview

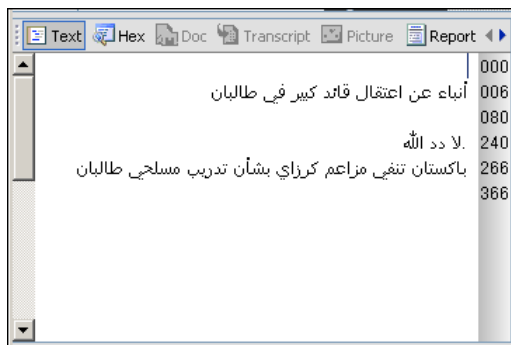
Encode Preview lets you apply text encoding to the Preview column on the Bookmarks and Search Hits tab. This feature allows non-English alphabet bookmarks and search hits to display properly in the Preview column.

### Turning On Encode Preview

The preview column displays certain non-English languages as plain text by default. When this happens, the text appears as a string of symbols that have no bearing on the actual text representation. Turning on Encode Preview displays the actual text using the proper characters.

Change the **Fonts > Tables** option to a Unicode font that supports the characters you intend to display. Arial Unicode MS is recommended because of the breadth of the characters included.

1. Open an evidence file and click **Text** or **Hex** in the View pane. The document appears.



2. Bookmark the desired passages (see *Bookmarking Items* (on page 401)).

3. Click **Bookmarks** on the Table tab of the Table Pane.

A preview of the bookmark appears.

Table   Report   Gallery   Timeline   Code			
	Bookmark Type	Preview	Comment
<input checked="" type="checkbox"/> 1	Search Summary		
<input checked="" type="checkbox"/> 2	Case Time Setti...		
<input checked="" type="checkbox"/> 3	Logs		
<input checked="" type="checkbox"/> 4	Highlighted Data	# F ( ' ! 9 F ' 9 * B ' D B ' & / C ( J 1 A J 7 ' D ( ' F	Arabic Unicode File

4. Right-click the desired bookmark and select **Encode Preview**.

<input checked="" type="checkbox"/> Encode Preview	
Summary Bookmark...	
Rename	F2
Show Columns...	
Column	▶
Sort	▶
Select Item	Space

The Table tab displays the Unicode in its proper form.

Table   Report   Gallery   Timeline   Code			
	Bookmark Type	Preview	Comment
<input checked="" type="checkbox"/> 1	Search Summary		
<input checked="" type="checkbox"/> 2	Case Time Setti...		
<input checked="" type="checkbox"/> 3	Logs		
<input checked="" type="checkbox"/> 4	Highlighted Data	عليه قر , افغانستان باعترقال احد كبار قادة حركة طالبان الملا دد الله. ب	Arabic Unicode File

## Indexing

Text indexing allows you to quickly query the transcript of entries. Creating an index builds a list of words from the contents of an evidence file. These entries contain pointers to their occurrence in the file.

There are two steps:

- Generating an Index
- Searching an Index

**Generating an Index** creates index files associated with evidence files. Index creation can be time consuming, depending on the amount of evidence you are indexing and the capabilities of your computer hardware. Evidence file size, and thus, the resultant index size is an important consideration when building an index. Attempts to index extremely large evidence files can have a serious impact on a computer's resources.

---

Note: For quicker index files, select a limited number of files for indexing.

---

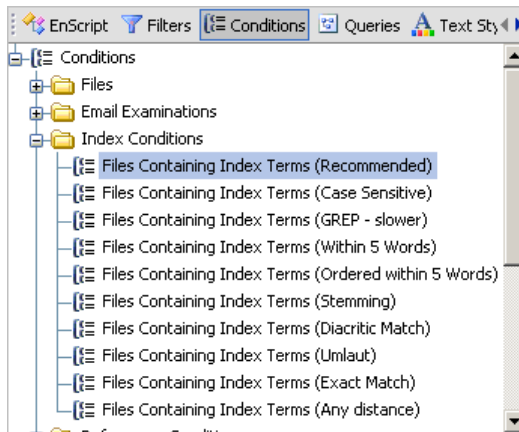
**Querying an Index** provides the means to search for terms in the generated index. Querying an evidence file's index for terms locates terms more quickly than keyword searching. The index is queried using several conditions accessed in the Conditions tab

## Querying an Index Using a Condition

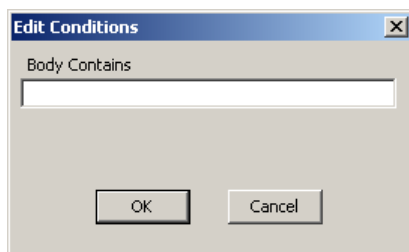
You can query the index using a condition.

- A Case must be created with Evidence files added.
- The evidence file must already have an index generated.

1. Display the **Conditions** tab of your interface, and expand the **Index Conditions** folder by clicking the + next to the folder.



2. Double-click on the condition you would like to use. All of the Index Conditions use the same dialog.



3. Enter the term you want to search for and click **OK**.

When complete, the Table pane lists files that meet the condition requirements.

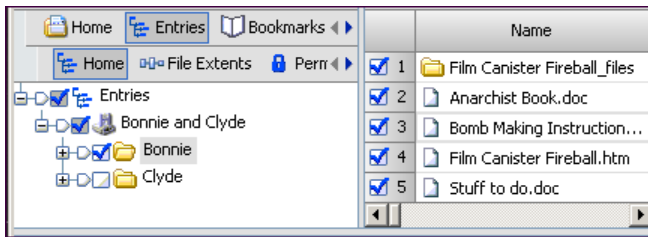
Table					
	Name	Filter	In Report	File Ext	File Type
<input checked="" type="checkbox"/> 1	Bomb Making Instruction...	Bomb Finder		htm	Web Page
<input checked="" type="checkbox"/> 2	Stuff to do.doc	Bomb Finder		doc	Word Document

The **Filter** column shows the condition that was run.

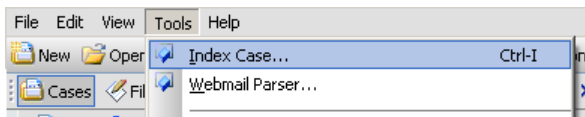
## Generating an Index

Open a case containing evidence files.

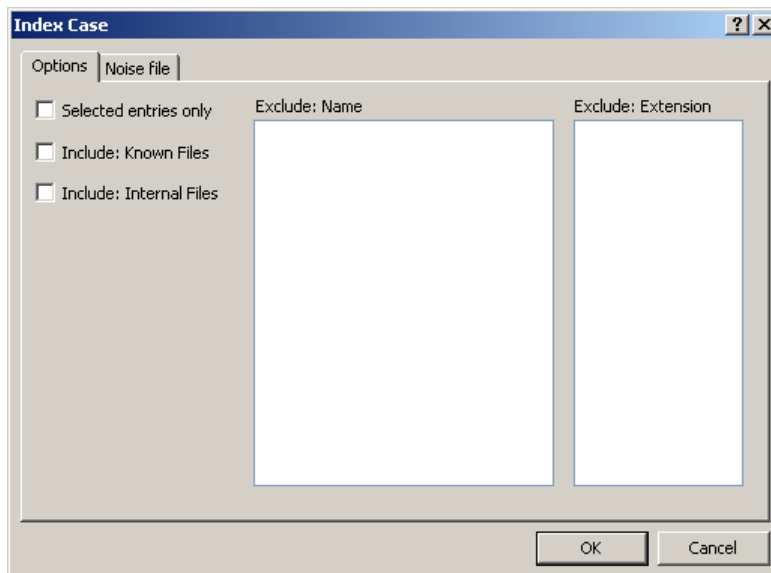
1. If you know the files you want to specifically index, select them in the Table pane.



2. Select **Tools > Index Case**.

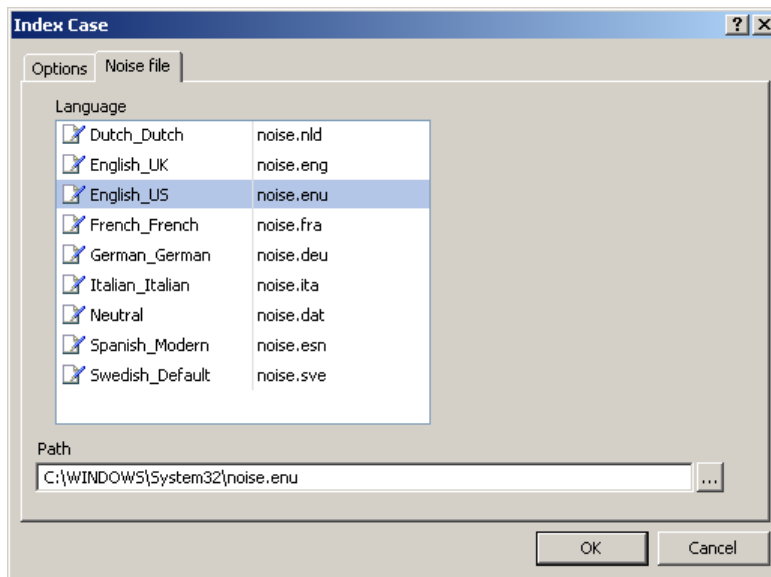


The Index Case dialog appears.



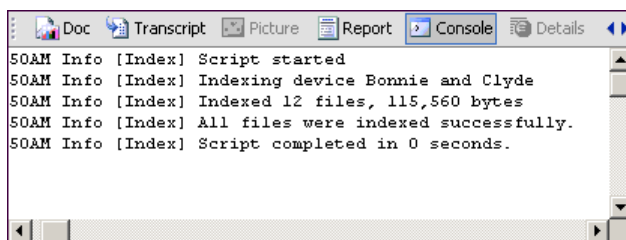
3. If you want only to index selected files, select **Selected Entries Only**.
4. If you want to include files with a known file signature, select **Include: Known Files**.
5. If you want to include internal files that are part of the NTFS file system, select **Internal Files**.
6. If you want to exclude any file names:
  - a. Right-click in the **Exclude: Name** list and select **New**.
  - b. Enter the name of the file and click **OK**.

7. If you want to exclude files by a particular file extension:
  - a. Right-click in the **Exclude: Extension** list and select **New**.
  - b. Enter the name of the file extension and click **OK**.
8. To set the noise file, click the **Noise File** tab.



9. Select the **Language File** and if necessary, modify the **Path**.
10. Click **OK**.

The Evidence file starts indexing. The thread bar indicates the estimated remaining time in the operation. The Console tab indicates diagnostic information as the index progresses.

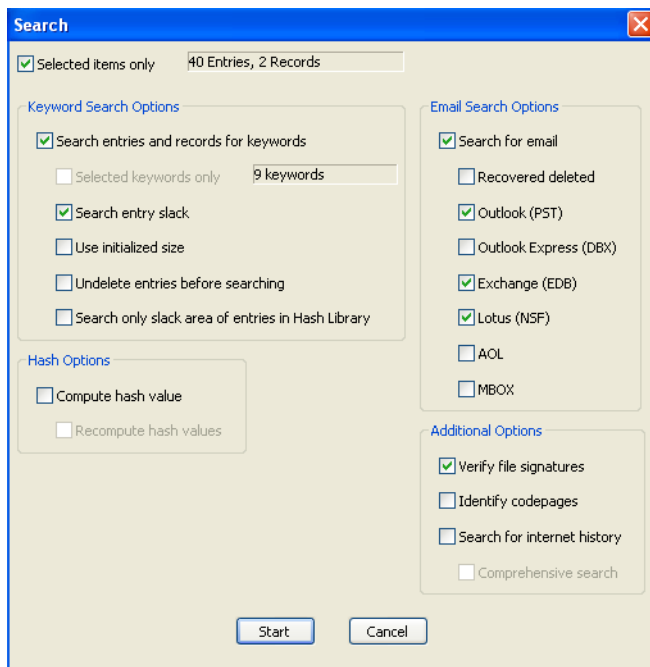


## Searching for Email

The program's search engine can search various types of email artifacts. This includes mail from:

- Outlook (.pst) (Outlook 2000 & 2003)
- Outlook Express (.dbx)
- Exchange (.edb) (2000 & 2003)
- Lotus Notes (.nsf) (5, 6, 6.5 & 7)
- AOL
- MBOX (Thunderbird)

1. In the Search dialog, select the desired Email Search Options.
2. Click **Start**.



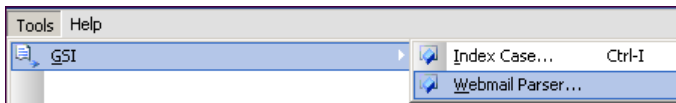
Note: In addition, clicking **Tools > GSI > Webmail Parser** specifically searches for Netscape®, Hotmail®, and Yahoo!® Web Mail.

## Web Mail Parser

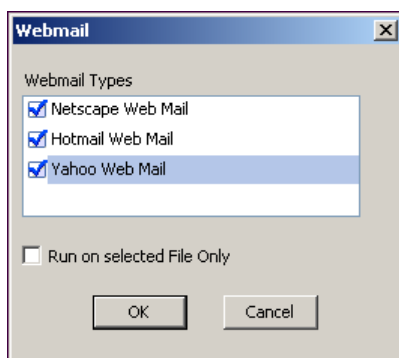
Web mail, including Netscape, Hotmail, and Yahoo Web mail can be searched.

Open a case that is thought to contain Webmail.

1. Select **Tools GSI > Webmail Parser**.



The Webmail parser options dialog appears.

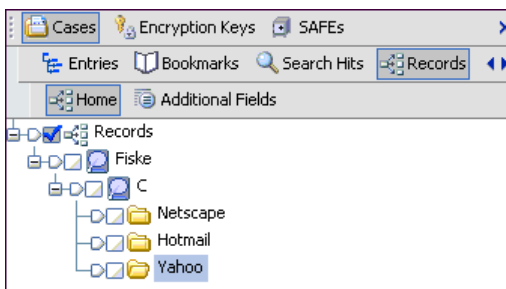


2. Select the Webmail types for collection. Optionally, a search can be run only on selected files. The search status displays on the status bar.



3. Click the Records tab.

The Tree pane displays a list of discovered files.



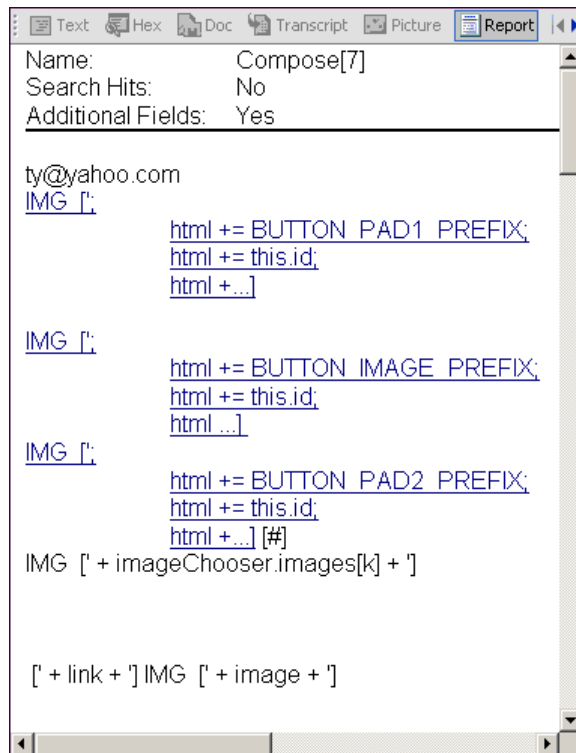
4. Open a folder to view its contents in the Table pane.

	Name	Additional Fields	Subject
<input checked="" type="checkbox"/> 1	242[1].htm	•	Re: FAKE ID, FAKE ...
<input checked="" type="checkbox"/> 2	95[1].htm	•	Re: Fake ID's
<input checked="" type="checkbox"/> 3	348[1].htm	•	Re: GO TO.... WW...
<input checked="" type="checkbox"/> 4	compose[1].htm	•	
<input checked="" type="checkbox"/> 5	mainentrance[1].htm	•	

5. To view the data in the Report pane, select a file and click Report.



File contents appear.



You can save or export the report as desired.

## Extracting Email

The program's search engine can search various types of email artifacts, including attachments.

See *Acquisition Wizard* (on page 198), *Performing a Search* (on page 357), and *Searching for Email* (on page 369) for additional information.

The procedures outlined in these sections discuss how to extract and view both email and attachments.

## Searching Email

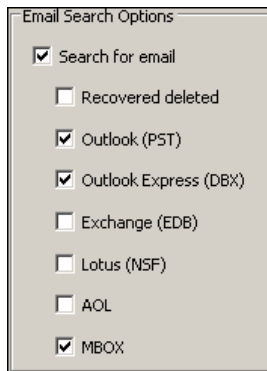
This program feature displays all emails and any associated attachments in tree view. Once recovered, these can be viewed in the Report, Doc, or Transcript tabs of the Report pane.

1. Click **Search**.



The Search page of the search wizard appears.

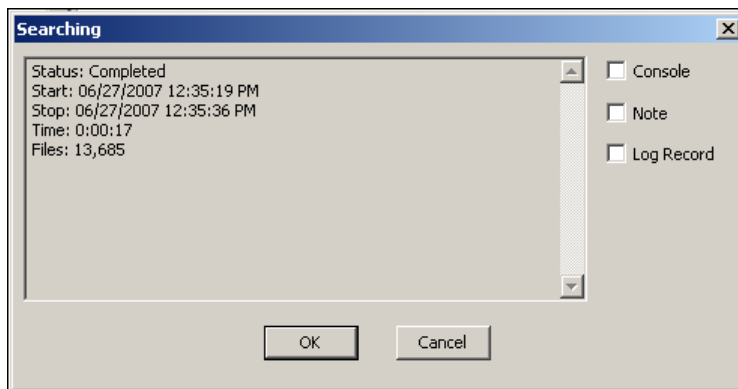
2. Select the desired email types and click **Start**.



View search progress in the status bar.



3. Click **OK** when the search complete dialog appears.
4. Click **Records**.



A closed tree view of all located mailboxes appears. Selecting a file displays one mail file's contents in the Text, Hex, Transcript, and Report tabs of the Report tab. In addition, the email file and its attachments are listed in the Table pane.

5. Open the high-level tree to see the mailbox's contents. Email contained in the mailbox is visible in the Tree pane, and both email and attachments are visible in the Report pane.

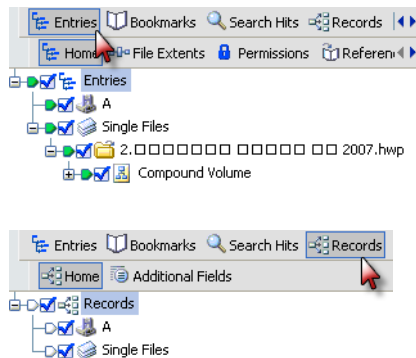
An envelope and paperclip icon indicates mail containing attachments.

After you finish, you can *view and interact with attachment* (see "Viewing Attachments" on page 374) files.

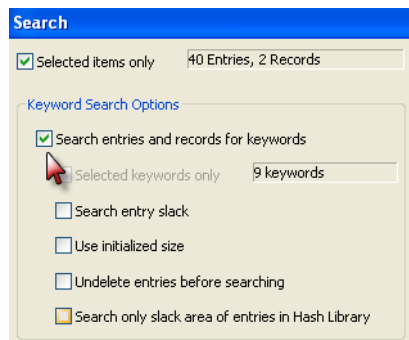
## Searching Selected Items

If you choose to search selected items, the items must be selected in both the Records and Entries tabs.

1. Blue check selected items in the Entries and Records tabs.



2. In the Search dialog under Keyword Search Options, click **Search entries and records for keywords**.



3. Click **Start**.

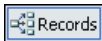
## Viewing Attachments

An email attachment is a file that is sent along with an email message. An attachment can be encoded or not.

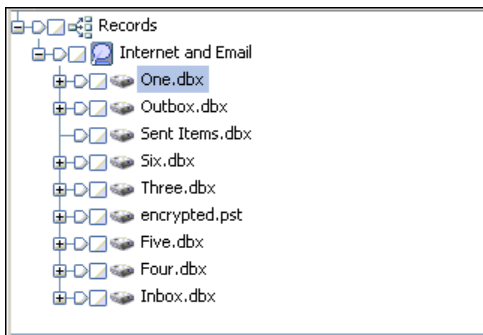
Complete a successful email search. See *Searching Email* (on page 371).

Email attachments clearly can have important evidentiary value. This section covers viewing attachments in their native format.

1. Click **Records**.

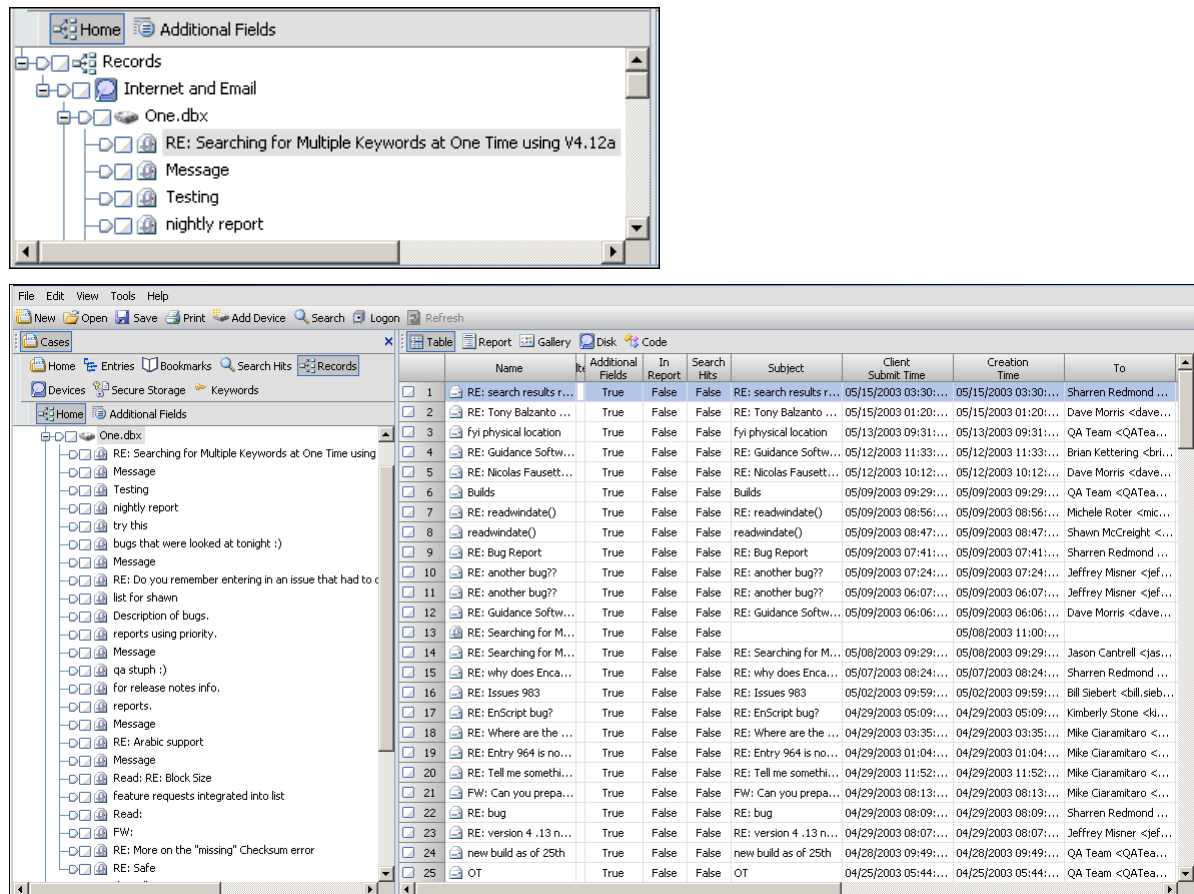


Discovered email appears in the Tree pane.



2. Expand the high-level item to view its contents.

A list of attachments appears in the Table pane and the contents of the attachment appear in the Report pane.



Emails and their attachments can be accessed and used for investigative purposes.

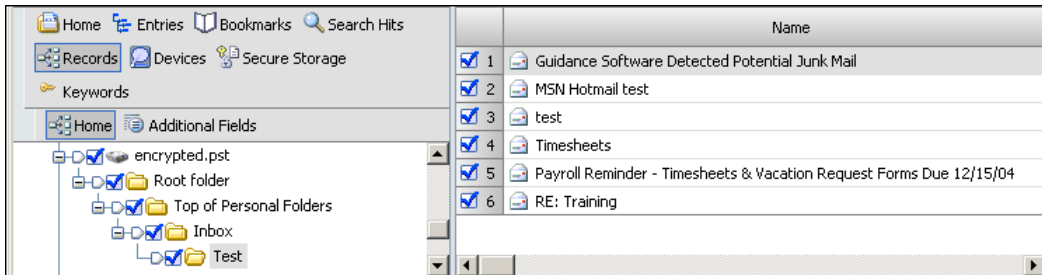
## Export to \*.msg

The Export to .msg option for mail files and mail files attachments lets you preserve the folder structure from the parsed volume down to the entry or entries selected. This option is available for the highlighted entry or selected items.

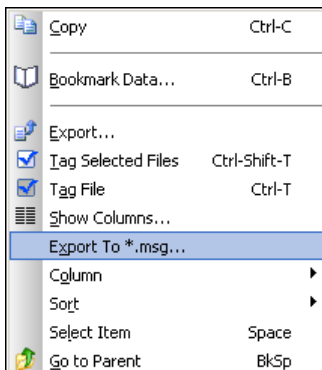
## Exporting to \*.msg

Perform an email search prior to executing **Export to .msg**.

1. Select an .msg file and display its mail contents.

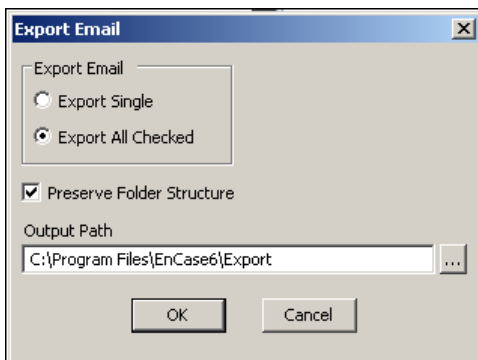


2. Select email files to export.
3. In the Report pane, select a file and right-click it.



4. Click **Export to \*.msg**.

The Export Email dialog appears.

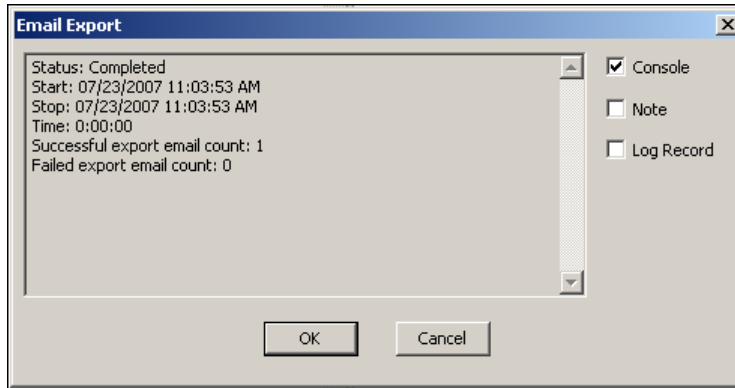


5. Select dialog options as needed:
  - ☐ **Export Single** exports only the selected message.
  - ☐ **Export All Checked** exports all files checked.
  - ☐ **Preserve Folder Structure** saves selected email folder structure information.

- ❑ **Output Path** captures the location of the export data file. The default is  
... \EnCase6\Export\.

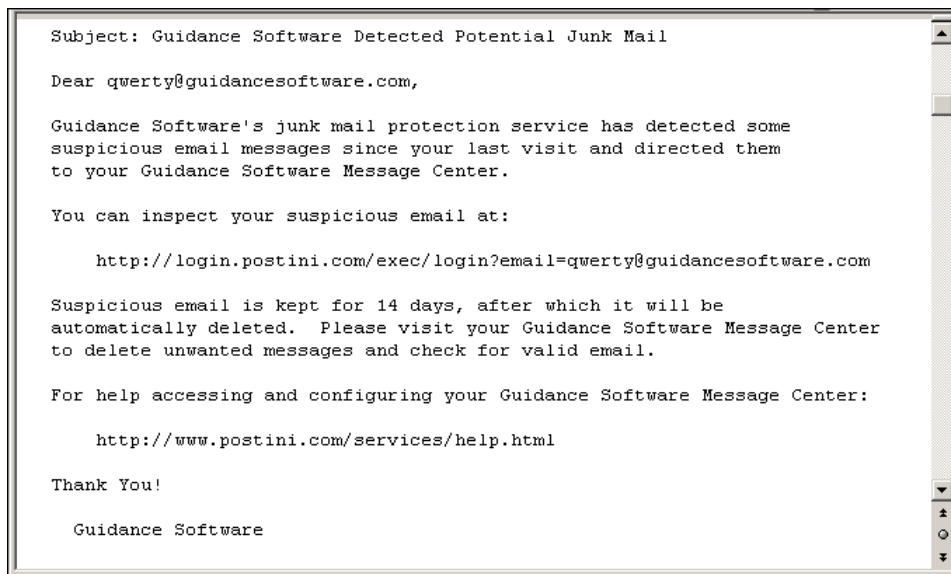
6. Click **OK**.

A message appears when the export function completes.



7. View the entire structure down to the individual message in the Export folder.
8. View a message by double clicking it.

The message text appears in read-only form. The figure shows a typical text message presentation.



## App Descriptors

At a very basic level, app descriptors are the hash files of a computer's EXE and SYS files. They work in conjunction with machine profiles and are used to identify forbidden or undesirable software on a computer's hard drive. They are particularly useful in detecting viruses and other malware and for ensuring a specified disk image is not changed.

The EnCase® program can identify malicious programs via a hash analysis. It compares an application's:

- unique digital identification
- its calculated, known, and stored hash value, with that captured in a snapshot.

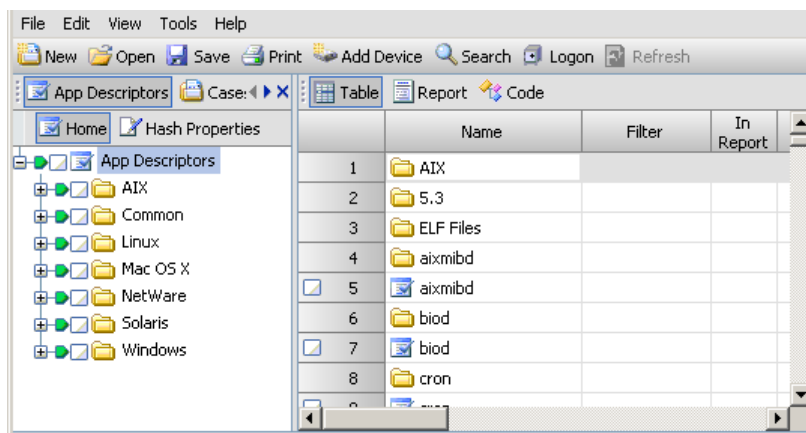
When the hash values match, the program returns the process name, its hash value, and machine profile to which it belongs. An app descriptor categorizes executables by hash value, to enable positive identification of executables running on a system.

App descriptors works in concert with machine profiles. Profiles are inventories of what should be running on a specific machine. Together, the machine profile and app descriptor lets an examiner know what should be running, and what is running on a specific computer.

## Manually Create App Descriptor

To run this feature, you must have created a machine profile and you must know the hash value of the file you intend to process.

1. Click **View > App Descriptors** to see a list of app descriptors.



2. Right-click a folder in the Tree pane or a file in the Table pane and click **New**.



A New App Descriptor dialog appears.

**New App Descriptor**

Name  
iTunes

Comment  
Shipping with OS X 10.4.8

Hash Value  
k435jk45j64h56g4567gikh56g7jk567

Machine Profiles

	Name	Comment	Allow
1	AIX 5.3		
<input checked="" type="checkbox"/> 2	Mac OS X 10.4.8		
3	NetWare 5.1 SP8		
4	NetWare 6 SP5		
5	NetWare 6.5 SP5		
6	Red Hat WS 3.0		
7	Solaris 8 32 bit		

OK Cancel

3. Complete these fields:
  - ☐ **Name** is mandatory, and is typically the name of the working file.
  - ☐ **Comment** is an optional field for investigator comments.
  - ☐ **Hash Value** is mandatory and must be entered manually. It contains the hash value of the selected file.
4. Select the machine profile in which to place the new app descriptor and click **OK**.

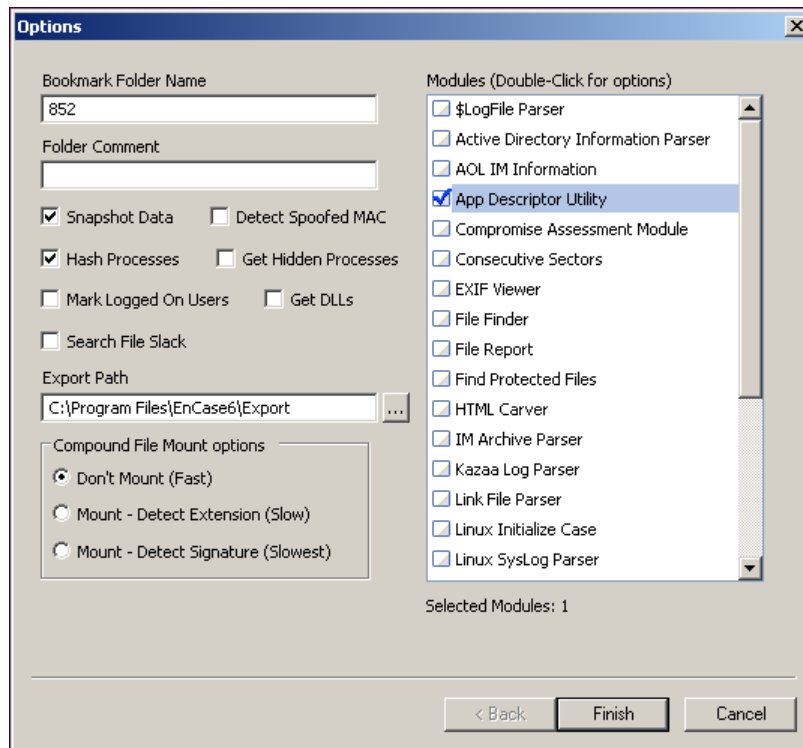
This method requires manual entry of the hash value for each and every new app descriptor. A far better and more efficient method is to use an EnScript program.

For information on automatically creating an app descriptor, See *Create App Descriptors with an EnScript Program* (see "Create an App Descriptor with an EnScript Program" on page 379).

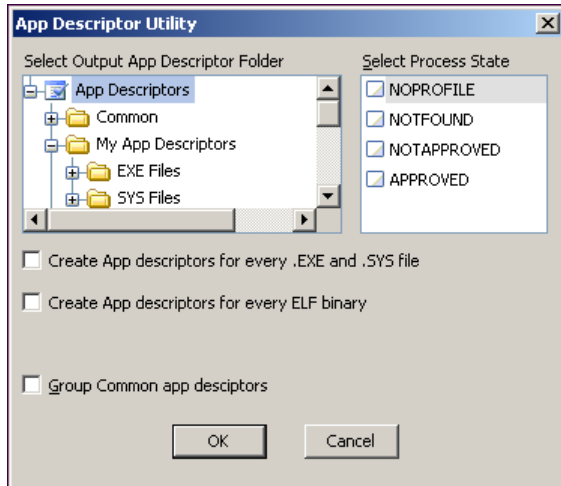
## Create an App Descriptor with an EnScript Program

The scripts for creating app descriptors are Scan Local Machine and Case Processor.

1. Run an EnScript program such as Scan Local Machine. An options wizard appears.



2. Complete the fields:
  - ☐ **Bookmark Folder Name** is the name of the folder in the bookmark area.
  - ☐ **Folder Comment** is an optional field for entering your own notes.
  - ☐ **Snapshot Data** is a mandatory checkbox.
  - ☐ **Hash Processes** is checked by default.
3. Click **Finish**.
4. Select, then double-click the App Descriptor Module to select an output file. If there are no folders displayed, create a new one.



Selecting a process state is optional. If either the **Create App Descriptors for every .EXE and .SYS file** or **Create App Descriptors for every ELF Binary** option is selected, Select Process State options are disabled.

5. Execute the selected EnScript program.  
When the script is complete, the newly created app descriptors are available.
6. Change the display as follows:
  - a. Click **Bookmarks**.
  - b. Double-click the new bookmark in the Tree pane.
  - c. Select **Snapshots** in the Table pane.
  - d. Select Snapshots tab. Select the Processes tab and the Home tab to view the information.
7. Select Include-All in the Table pane to view the name, hash value, and app descriptor data for the files.

## Encryption Support

Encryption is the process of converting data into a format that cannot be read by others.

Encryption is used to protecting information in many kinds of systems, including computers, networks, the Internet, mobile telephones, and so forth.

EnCase has the ability to decrypt a variety of encrypted documents including those using symmetric and asymmetric keys. The commercial encryption keys that EnCase currently supports includes Lotus NSF, PC Guardian Encryption Plus, PC Guardian Encryption Plus, Utimaco Safe Guard Easy, Credant, and SafeBoot.

## NSF Encryption Support

The Lotus Notes email client has security built into the product. Notes was the first widely adopted software product to use public key cryptography for client-server and server-server authentication and for encryption of data, and it remains the product with the largest installed base of PKI users.

The EnCase® Suite can decrypt encrypted NSF documents and send them to recipients within the same Domino server.

Each server user has an ID file that contains a user's:

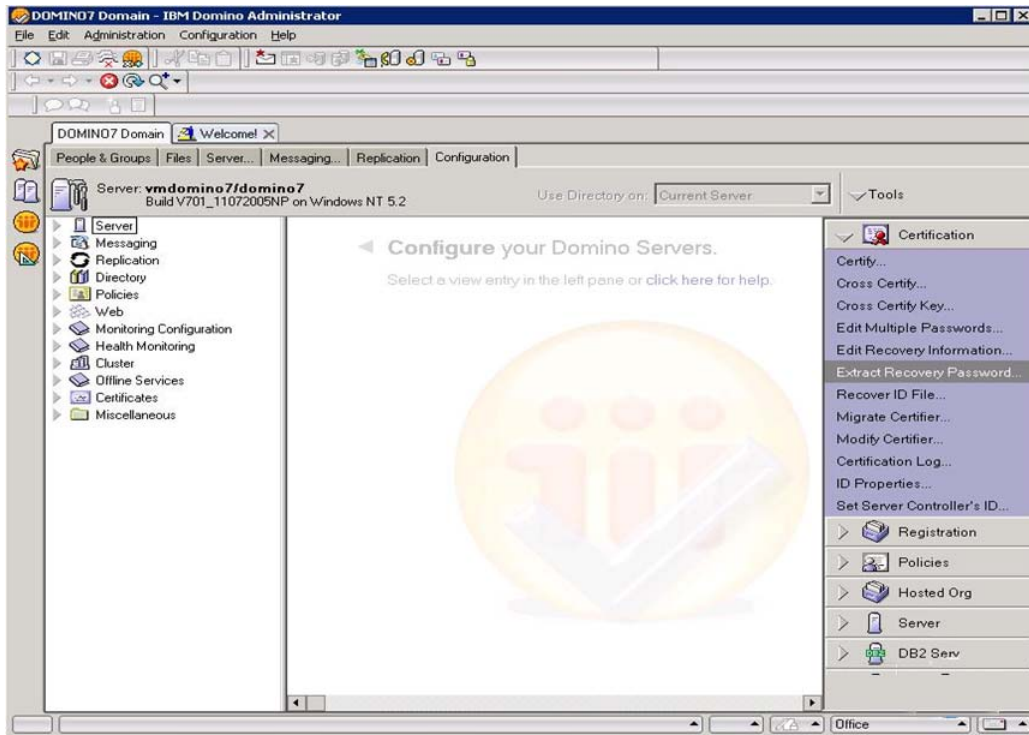
- encrypted private key
- public key
- password information
- password recovery information

It also has an NSF file that represents the user's mailbox in 8.3 format in the default path `<domino installation folder?\data\mail\<user>.nsf`.

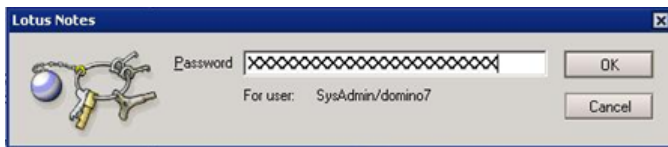
## Recovering NSF Passwords

To retrieve the recovery password, you must have proper administrative rights on the Domino server.

1. Open the Domino Server.

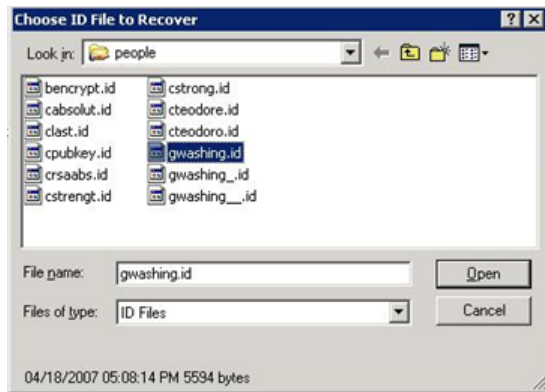


2. Log in as the server administrator.



3. Click OK.

The password ID list appears.



4. Click **OK**.

The recovery password appears.



5. Click **OK** and define users authorized to generate recovery passwords.

## Disk Encryption Support

This feature provides the ability to view and parse encrypted disks and files protected by PC Guardian Edge Encryption Anywhere™, PC Guardian Edge Encryption Plus, or Utimaco SafeGuard Easy in both 32 and 64 bit systems.

After previewing the encrypted device or to acquire it to an evidence file, you need the target's user name, password and domain to parse the disk in EnCase.

A message box displays asking for the user ID, password, and domain. If this information is unavailable, you can still view the volumes in the Tree pane, but the contents remain encrypted.



The Domain can be a DNS name.

Once a Logical Evidence File or a new Physical Disk is added to a new case, the master boot record is checked against known signatures to determine if the disk is encrypted or not. If the disk is encrypted, you are asked for user credentials which consists of username, password, and domain. When these are entered, the disk is decrypted.

---

Note: Utimaco and PC Guardian need only a user ID and a password. The domain name is unnecessary.

---

After successful parsing of an encrypted evidence the symmetric encryption key is stored in the case once the case is saved. When this case is reopened the user is not asked to provide credentials and the decryption is done using the stored key.

## SafeBoot Setup

EnCase provides a way for you to view SafeBoot-encrypted hard drives during an investigation. Prior to any decryption however, the SafeBoot installer, available from Guidance Software Technical Support Support Portal (<https://support.guidancesoftware.com>), must be installed. This section describes that process.

The following files and folders are included in the SafeBoot installer file.

1. Unzip the file's contents to C:\Program Files\EnCase6\Lib\SafeBoot Technology\SafeBoot directory of the EnCase install directory.

---

This is the default path and directory. You may change it, if necessary.

---

File / Folder Name	MD5 Hash	SHA-1 Hash
<u>sb\Logs</u> folder [blank]		
<u>sb\Tokens</u> folder		
<u>SafeBoot</u> Tool folder		
SbAdmDll.dll	78659b65f2ac4ebcb280d15a0954a274	ceab3b1b66484b84d51e6583a6b7c224db109379
SbComms.dll	7cc991691c16593cb6096a4343b7a0f5	fe6012501533a80d9d4a316ae642f0544c59ad06
SbDbMgr.dll	5ef7c0de3942a116b4e9779382ea9f27	4be95a4eea760e9814e86679e0aa15138a1a7950
<u>SbErrors.xml</u>	af495a2020da74a34063080724b996ce	712f97381235210dae61f110672f88a20f474311
SbFileObj.dll	2dfc5f1b9947f54e88cdaff1e9c93c4	ba065677f86e107026aa8623dfc11477e542d8ee
SbGroupObj.dll	cae95d17e1b9f24a0b380a51784883d9	c143a650a4f6ac59eca4dbcb8a505202b563561b
SbMachineObj.dll	d1b604432d48bb94e9217734e50ac9bd	3a50382c2a2fd385bb4920ceee687b8b72667c08
SbUiLib.dll	f0f07cec0420083206a7252020767802	2f69189ea4991e73ac7df300dc4dc6d7f61fc9da
SbUserObj.dll	4643f5f3ca93a3995b0d9b385a0be092	c0e41b68f98c676bba17c718bb8b8b0c2afba3d7
SbXferDb.dll	8f95dd835c58f5c54ef234d41eac8934	flfc45d17317a3f25d7b18970a2b93ed1a872f34
<u>SafeBoot</u> Tool\GetKey Offline.xml	6eb533c9084280cbf28c7123351cb786	626ff63013af6feda593820d711a64af350f426fb
<u>SafeBoot</u> Tool\GetKey Online.xml	09059cb56947364d3e675b4901a89093	3e1797a1e72c91991a94f00641fc445abc544025
<u>SafeBoot</u> Tool\SafeBootTool.exe	40dd4495fa5003478feb33af73c6446a	9c7f1ae0a4c4b1cc1f32a62a9d9770627d427119
sb\Tokens\SbTokenPwd.dll	0f60b78d7cfcb8a5a318ca6741903161	40130899b6c0d0314c68489b30d67cd4b863db8e

2. Copy the files shown here from the server to the appropriate location. The table assumes the server installation is c:\program files\sbaadmin.

Additional SafeBoot installation files:

Copy from:	Copy To:
C:\Program Files\SBAdmin\SDMCFG.INI	C:\Program Files\EnCase6\Lib\SafeBoot Technology\SafeBoot
C:\Program Files\SBAdmin\ALGS\<Algorithm>\SbAlg.dll	C:\Program Files\EnCase6\Lib\SafeBoot Technology\SafeBoot\sbAlgs

## Exporting a Machine Profile from the SafeBoot Server

Before you can perform an offline decryption of a SafeBoot-encrypted drive, you first need to export the target machine profile from the SafeBoot server.

Here are the steps to accomplish an offline machine profile.

---

Be sure that you have obtained the SDMCFG.INI and SbAlg.dll files from the SafeBoot Server as described in **SafeBoot Setup** (on page 385) .

---

1. Log on to the SafeBoot server with an administrator account.
2. Launch SafeBoot Administration Tools from **Start Menu→Programs→SafeBoot Administrator Tools→SafeBook Administration**.
3. Log in with the SafeBoot administrator account.
4. Click the Device tab.
5. Expand the SafeBoot Machine Group tree.
6. Double-click on the SafeBoot Machine child in the SafeBoot Machine Group tree.

A list of all computers registered to this particular SafeBoot database appears on the right side of the SafeBoot Administrator screen.

7. Right-click the computer name you wish to decrypt, then select **Export Configuration** from the menu.

The Export Configuration screen displays.

8. Click **Browse** to specify the SDB file's storage location.
9. We recommend using the computer name as the SDB file name.
10. On the Export Configuration screen, select **Include all users in the configuration**, then click **OK**.

An Export Configuration dialog displays.

11. Repeat steps 7-10 for all other computers you want to decrypt.



## Authentication

### Modify the SDMCFG.INI File

Before performing an online authentication, modify the file from the SafeBoot server:

1. Open `SDMCFG.INI` file with a text editor and, if the line exists, change the value of **AuthType=1** to **AuthType=0**.

If AuthType is set to 1, communication between the SafeBoot server and EnCase is encrypted and the online authentication process is hindered.

2. If the line does not exist in the file, enter **AuthType=0** to the end of the file.

## SafeBoot Encryption Support (Disk Encryption)

EnCase provides a way for you to view SafeBoot-encrypted hard drives during an investigation. This feature is only available to a user with an EDS cert enabled.

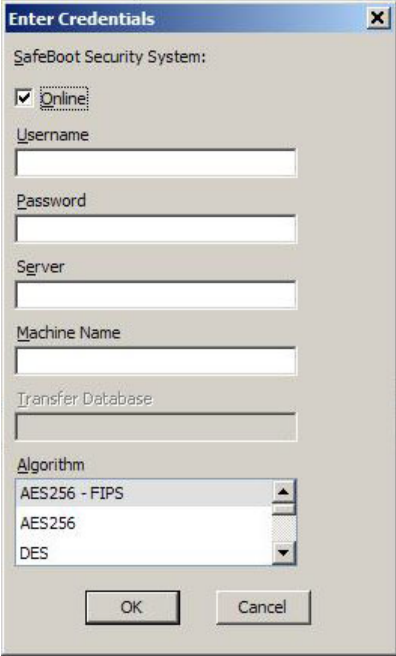
---

Note: If no EDS cert is found, the physical device will mount, but the encrypted file structure cannot be parsed.

---

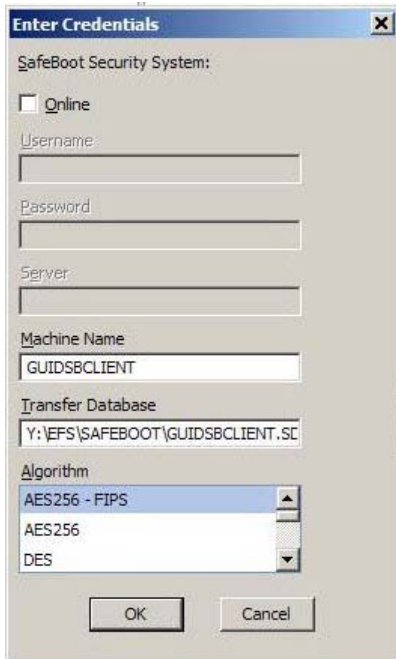
*Use EnCase to perform SafeBoot Encryption as follows:*

1. Use the Add Device Wizard to add the device or volume.
2. When prompted, select the appropriate encryption algorithm from the list, then enter a user name, server name, machine name, and password when in online mode.



The SafeBoot encrypted drive will be parsed.

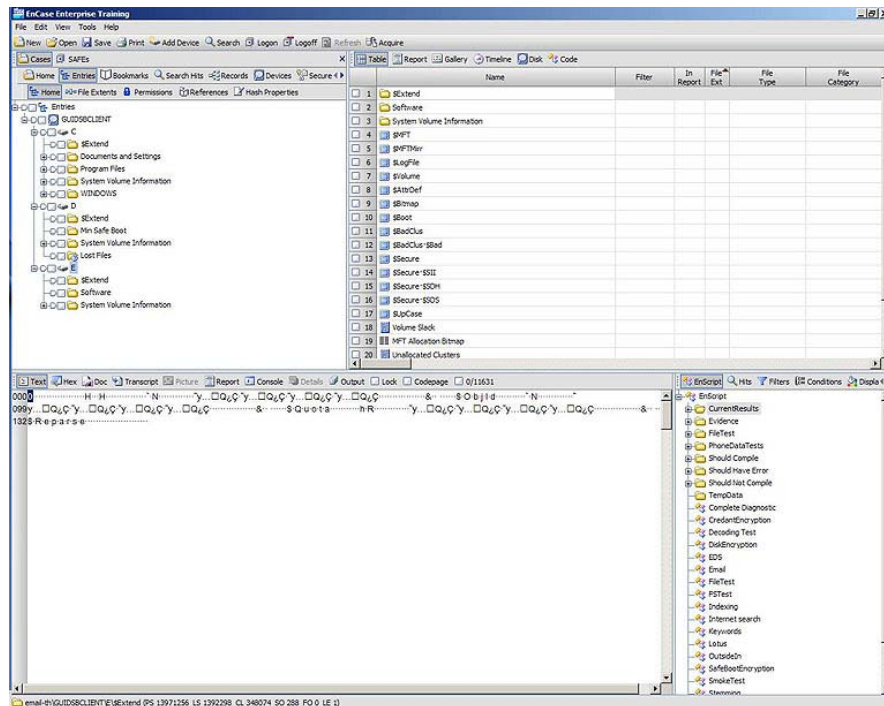
The offline dialog is similar. The Online check box is blank and only the Machine Name, Transfer Database field, and Algorithm are available:



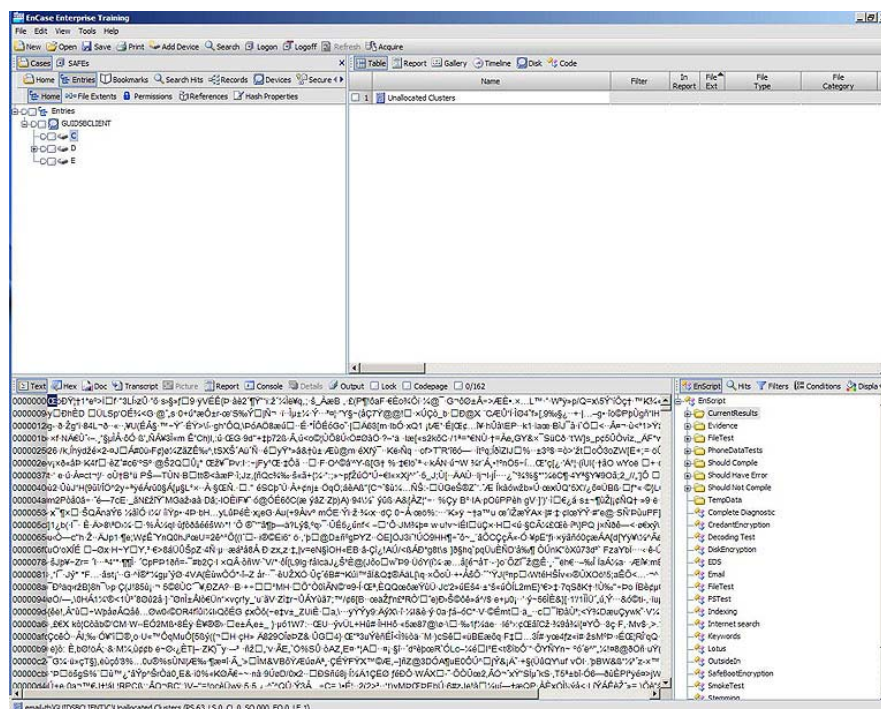
The screenshot shows a Windows-style dialog box titled "Enter Credentials". Inside, under the heading "SafeBoot Security System:", there is an unchecked checkbox labeled "Online". Below this are three text input fields: "Username:", "Password:", and "Server:", all of which are currently empty. Further down are two more text input fields: "Machine Name" containing the text "GUIDSBCLIENT" and "Transfer Database" containing the text "Y:\EFS\SAFEBOOT\GUIDSBCLIENT.SC". Below these is a dropdown menu labeled "Algorithm" which is currently open, showing three options: "AES256 - FIPS" (which is highlighted in blue), "AES256", and "DES". At the bottom of the dialog are two buttons: "OK" and "Cancel".

3. Save the case once a successful decryption is complete. The credentials entered in the dialog are stored in Secure Storage, eliminating the need to enter them again.

This illustration shows results of a successful decryption. The Tree pane shows a SafeBoot folder, the Table pane contains a list of decrypted files while the Text pane shows contents of a decrypted file.



4. The next figure shows the same files as they appear encrypted.



## Supported SafeBoot Encryption Algorithms

EnCase's SafeBoot decryption feature supports these encryption algorithms:

- AES256 FIPS
- AES256
- DES
- RC5 - 12 Rounds
- RC5 - 18 Rounds

## CREDANT Encryption Support (File-Based Encryption)

EnCase provides a way for you to access CREDANT-encrypted data on Windows devices.

---

You can obtain the CREDANT API installer from CREDANT Technical Support (<http://www.credant.com/>).

---

EnCase reviews your mounted files and looks for CREDANT-encrypted data. If it finds this data, a logon dialog displays.

1. The dialog populates with a known user name and password, Server, Machine ID, and the Shield CREDANT ID (SCID). CREDANT files are processed and decrypted with no further interaction.

CredentV5.2.1.163\_BlowFish\_HD

Credant Mobile Guardian credentials:

☒ Online

Username

Password

Server

https://10.0.40.68:8081/xapi

Offline Server File Path

Machine ID

tt-vm1-Email.Credent.local

Shield CREDANT ID

CI7M22CU

OK Cancel

The offline dialog is similar. The Online check box is blank and the Machine ID and SCID fields are unavailable.

CredentV5.2.1.163\_BlowFish\_HD

Credant Mobile Guardian credentials:

☐ Online

Username

Password

Server

https://10.0.40.68:8081/xapi

Offline Server File Path

Machine ID

tt-vm1-Email.Credent.local

Shield CREDANT ID

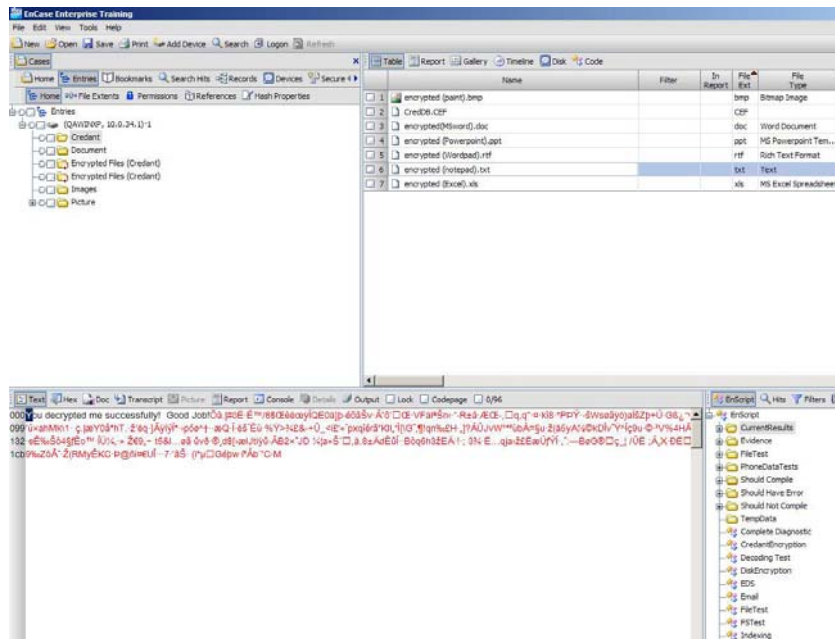
CI7M22CU

OK Cancel

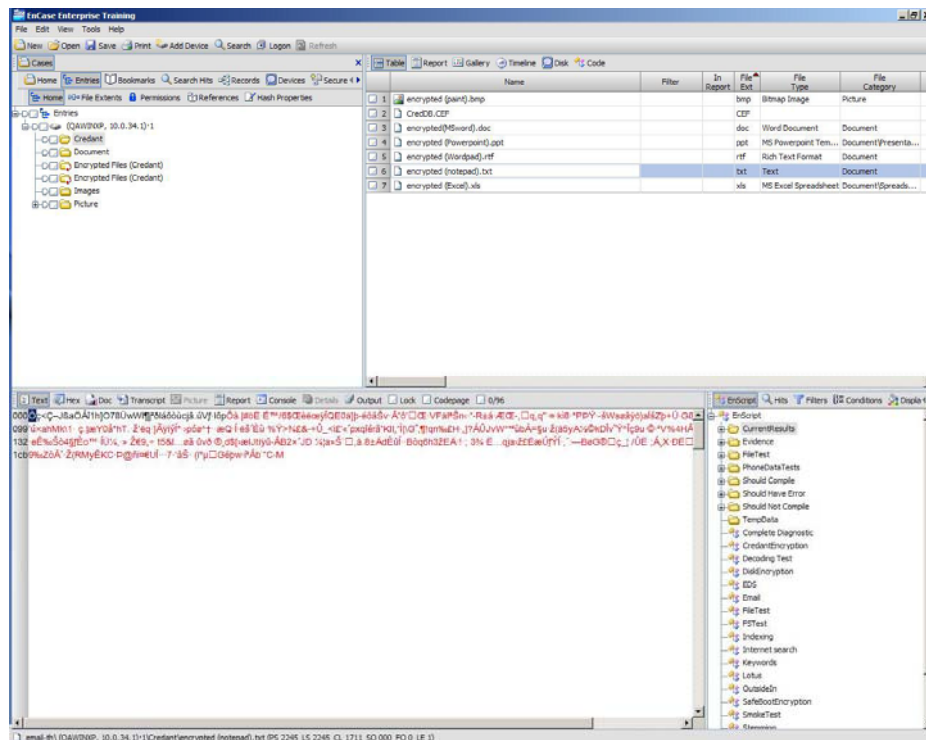
2. Save the case once a successful decryption is complete. The credentials entered in the dialog are stored in Secure Storage, eliminating the need to re-enter them.

The illustration below shows results of a successful decryption:

- The Tree pane shows a CREDANT folder
- The Table pane contains a list of decrypted files
- The Text pane shows contents of a decrypted file



The next illustration shows the same files as they appear unencrypted.



## Supported Encryption Algorithms

EnCase's CREDANT decryption feature supports these encryption algorithms:

- AES128
- AES256
- 3DES
- Rijndael 128
- Rijndael 256
- Blowfish

## CREDANT Encryption Support (Offline Scenario)

If the machine to be investigated is not on the network with the CREDANT server, you must obtain the CREDANT keys and store them in a location accessible to the Examiner machine.

Before you begin:

You must install the CREDANT Library Installer to run the utility with the appropriate DLLs. You can obtain the installer from CREDANT technical support.

You must have EnCase Decryption Suite installed on the Examiner dongle that will decrypt the CREDANT-encrypted data.

You must obtain the URL for the CREDANT Mobile Guardian (CMG) Device Server.

You must obtain the Administrator username and password. The CREDANT administrator must have Forensic Administrator privileges, as specified in the CMG Server Web Interface for CMG v5.4 and later servers. The administrator must have Security Administrator privileges for the v5.3 server.

You must obtain the Administrator's login domain (for CMG 6.0 and later servers only), the Machine ID for the target device (MUID), the Shield CREDANT ID (SCID), the Username that the key material is being downloaded for, and the Password to use to encrypt the output .bin file.

1. At a computer that has communication to the CREDANT Server, run the utility CEGetbundle.exe from the Windows command prompt. CEGetBundle.exe is supplied by CREDANT in the CREDANT Library Installer, which also installs the DLLs necessary for the decryption. Copy the DLLs and MAC file to the target device as well.

2. Supply the parameters as follows: CEGetBundle [-L] XURL -aAdminName -AAdminPwd [-DAdminDomain] [-dDuid] [-sScid] [-uUsername] -oOutputFile -oOutputFile -IOutputPwd

-L	Legacy mode for working with pre 5.4 server installs
URL	Device Server URL (e.g., <a href="https://xserver.credant.com:8081/xapi">https://xserver.credant.com:8081/xapi</a> )
AdminName	Administrator user name
AdminPwd	Administrator password
AdminDomain	Administrator domain (optional: required only if the CMG Server is configured to support multiple domains)
MUID	Machine ID for the target device (also known as the Unique ID or hostname)
SCID	Shield CREDANT ID (also known as DCID or Device ID)
Username	Name of the forensic administrator
OutputFile	File to save the key material in
OutputPwd	Password to encrypt output file

Here is a command example: `cegetbundle -L -X"https://CredantServer:8081/xapi" -a"Administrator" -Achangeit -d"CredantWorkstation.Credant.local" -sCI7M22CU -u"Administrator" -o"C:\CredantUserKeys.bin" -iChangeIt`

3. Place the .bin file downloaded from the CREDANT server in a path accessible from the Examiner machine. Open EnCase and create a new case or open an existing one. You must have EnCase Decryption Suite installed on the Examiner machine that decrypts the CREDANT-encrypted data.

---

**Note:** In legacy mode, you must execute this utility for each user targeted for investigation on the target device while specifying the same output file. The keys for each user are appended to this output file.

---

4. Acquire a device with CREDANT encrypted files, or load an evidence file into the Case. The Enter Credentials dialog displays, prompting you for only the Username, Password, Server/Offline Server File, Machine ID, and Shield CREDANT ID (SCID) information.

---

**Note:** In Offline mode, the only information you must provide is the Password and Server/Offline Server File (full path and filename to the .bin file downloaded using the CEGetBundle.exe utility).

---



When EnCase decrypts CREDANT encrypted files, the key information is placed in Secure Storage in EnCase, and saved with the case. You do not have to re-enter this information.

## Enabling the Forensic Administrator Role on the CREDANT Server

To enable the Forensic Administrator role on the server, you must change settings as described below.

---

These instructions assume that the CREDANT installation folder is **C:\Program Files\CREDANT**.

---

1. Enable the Web interface for EnCase to download the encryption keys:
  - a. Open **C:\Program Files\CREDANT\CMG Enterprise Edition\Device Server 1.2\conf\context.properties**.
  - b. Make sure the forensic method is enabled: **service.forensic.enable=true**.

Stop and restart the device server from the Start menu:

Click **Start→CMG EE→Device Server→Stop Device Server Service**, then **Start Device Server Service**.

1. Add the Forensic Administrator role:
  - a. Open **C:\Program Files\CREDANT\CMG Enterprise Edition\Server Web Interface 5.4\conf\context.properties**.
  - b. Enable the Forensic Administrator type: **admin.type.forensic=true**.
  - c. From the Start menu, stop and restart the server Web interface.

The new role shows in the place where you configure administrator accounts.

## S/MIME Encryption Support

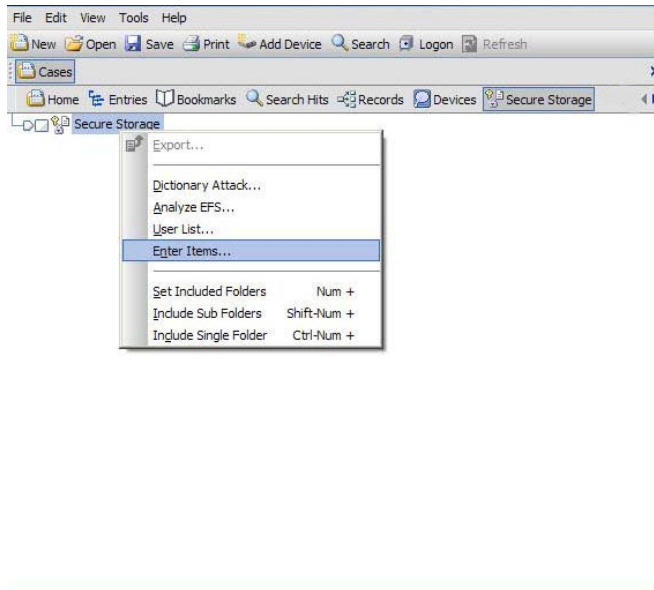
The EnCase S/MIME Encryption Support provides the ability to decrypt S/MIME-encrypted emails found in PST files. Email sent or received with the file extensions .pst, .mbox and .edb support the S/MIME PKCS #7 standard.

The mail attachment must meet the PKCS 12 standard, and you must have PFX certificates installed. PST, EDB, and MBOX mail containers are supported.

*To decrypt S/MIME data:*

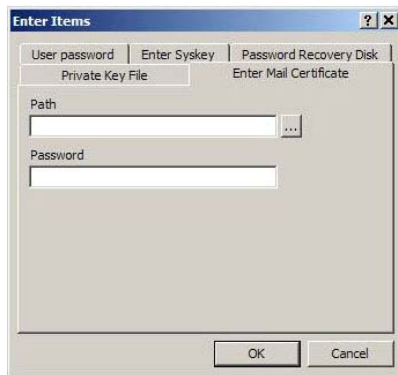
1. Open or create a case and enter Secure Storage.
2. Right-click on a folder in the left pane.

A drop-down menu displays.



3. Select **Enter Items**.

The Enter Items dialog displays.



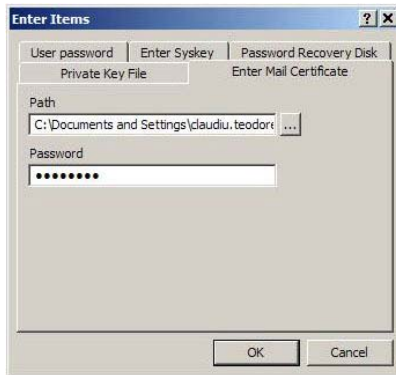
4. Select the Enter Mail Certificate tab.

---

The only allowed certificate format is .PFX.

---

5. Enter the path to the PFX certificate and the password, then click **OK**.

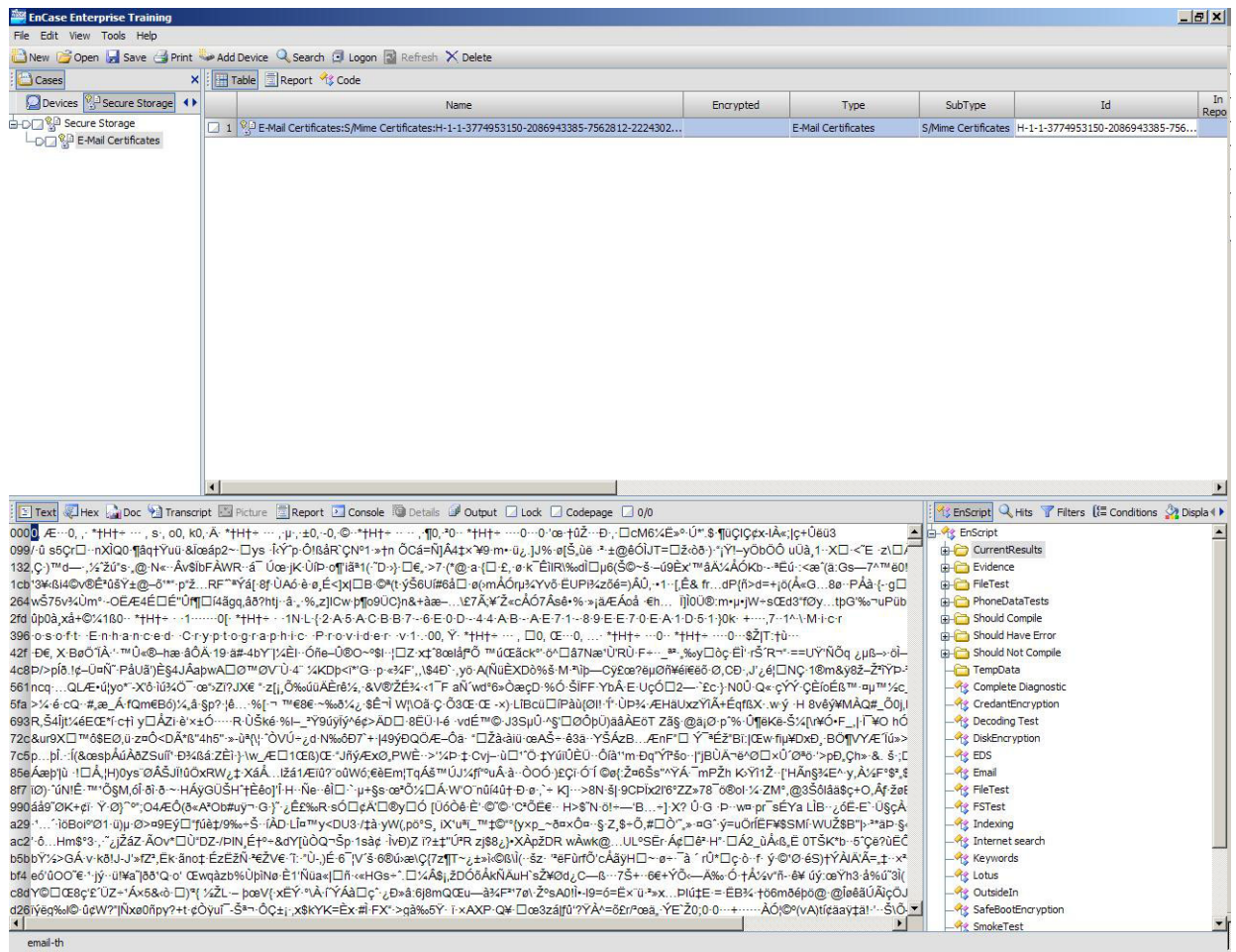


The PFX cert is decrypted and stored in Secure Storage.

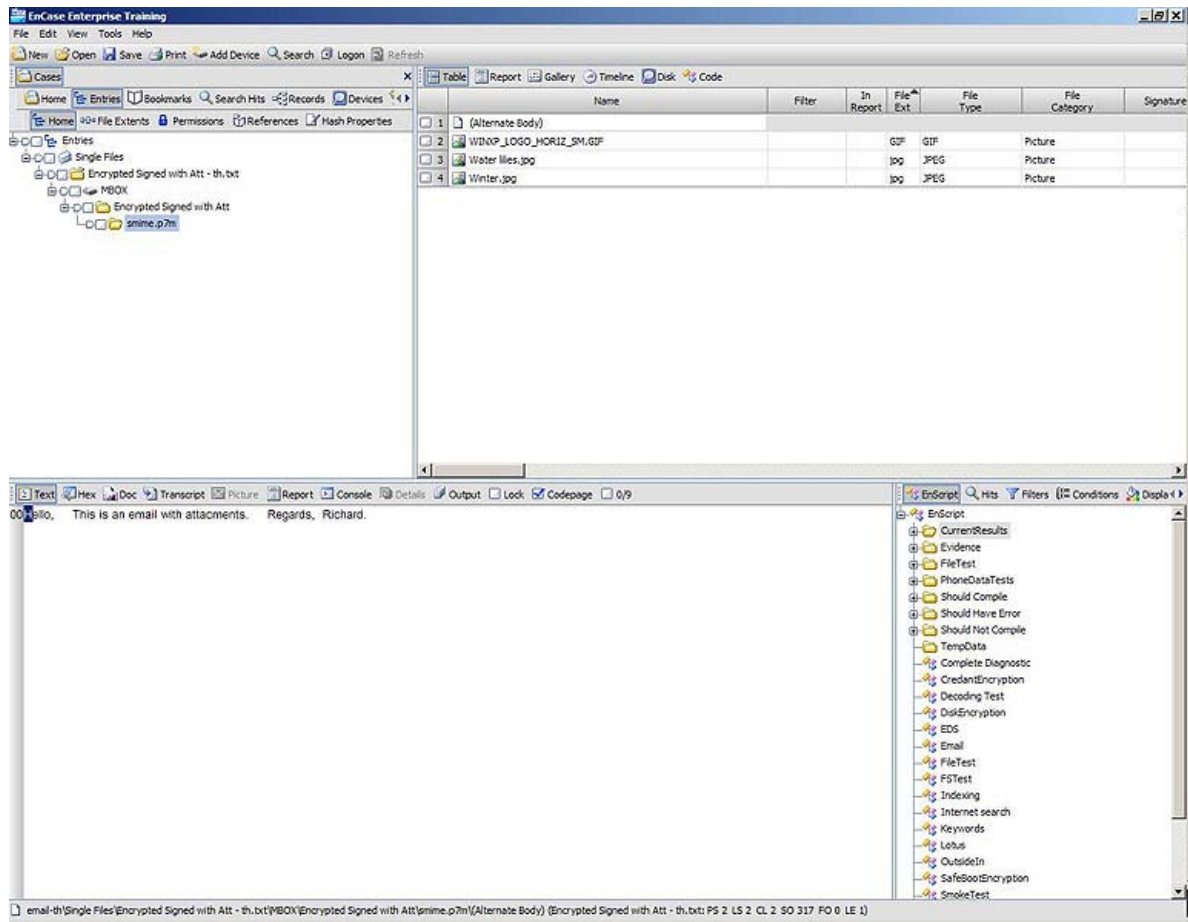
S/MIME decryption and signature verification happens in background.

Given the proper password, the certificate is stored in Secure Storage under E-Mail Certificates folder. After you import the required certificates into Secure Storage, you can parse the email container files using the View File Structure feature in the Entry View.

S/MIME contents are displayed like this prior to decryption:



When parsing is complete and successful a directory list displays. In the illustration, the folder is entitled smime.p7m. The text of the email is shown in the Text pane while the email's attachments appear in the Table pane. You should view and work with content in the Records tab.



## EFS Files and Logical Evidence (LO1) Files

To decrypt an encrypted EFS file you need the following:

1. The EnCase EDS module
2. The \$EFS stream. This is essential, since it contains the decryption key.
3. A matching unencrypted private key. This can be the recovery agent's key or a user's key.
4. File slack might be needed if the file size is not a multiple of 16. This is because files are decrypted in 16-byte chunks.

---

For example, a 17-byte file needs 15 bytes of slack in order to decrypt the last chunk. Otherwise, only multiples of 16 are decrypted.

---

In EnCase version 6.11, there are different scenarios from prior versions when adding EFS files to a logical evidence (L01) case:

The file is *encrypted* and the *\$EFS stream is missing from the same folder* within the L01: **the file cannot be decrypted.**

The file is *encrypted* and the *\$EFS stream is in the same folder*: **the file can be decrypted** (except for the remainder of the file, if any).

The file is *decrypted* and the *\$EFS stream is missing*: **the file remains decrypted.**

1. The file is *decrypted* and the *\$EFS stream is in the same folder*: **the file will be decrypted twice.**

---

The workaround in this case is to disable EFS or delete the private key from the secure storage.

---

From version 6.11 on, all the scenarios above are handled gracefully, because the \$EFS stream is added internally.

- If the file is encrypted, the \$EFS stream is automatically stored with the file as metadata.
- If the file is decrypted, the \$EFS stream is not automatically stored, as it is not needed. This does not prevent you from storing the stream by specifically saving it to the LEF.

---

If an encrypted file is decrypted and added, this is noted and displayed in the report.

---

# Bookmarking Items

- Bookmarks Overview 401
- Bookmark Features 406
- Creating a Bookmark 414
- Using Bookmarks 422

## Bookmarks Overview

EnCase allows files, folders, or sections of a file, to be marked and saved for reference. These are called bookmarks. Bookmarks are stored in their associated case file and can be viewed any time by selecting the Bookmarks tab. You can mark any existing data or folder.

---

Note: When a file is initially written to a multi-session CD it is assigned an address offset. When the file is changed, it is written again to the CD as a new file but with the same offset. Any revisions to this initial file are all assigned the same offset.

---

The file, and all its revisions can be viewed.

---

EnCase provides the following bookmark types:

- Highlighted data
  - ☐ Annotates selected data
  - ☐ Also referred to as sweeping bookmarks
- Notes
  - ☐ Allows the user to write additional comments into the report
  - ☐ Provides some text formatting capabilities
  - ☐ Not bookmarks of evidence
- Folder information and structure
  - ☐ Annotates the tree structure of a folder or the device information of specific media
  - ☐ No comment feature
  - ☐ Options include showing device information, such as drive geometry, and the number of columns to use for the tree structure
- Notable File
  - ☐ Annotates individual files
  - ☐ Fully customizable
- File group
  - ☐ Annotates groups of selected files
  - ☐ No ability to comment
- Snapshot
  - ☐ Contains the results of a System Snapshot of dynamic data for Incident Response and Security Auditing



- Log record
  - Contains results from log parsing EnScript programs
- Datamark
  - Contains the results of Windows registry parsing EnScript programs
- Case time setting
  - Shows whether Daylight Savings Time is being used on the evidence file and whether dates should be converted to a single time zone
- Search summary
  - Contains search results, times, and keywords for a particular case

---

Note: Case time settings bookmarks and Search summary bookmarks are created automatically.

---

## Highlighted Data Bookmarks

The highlighted data bookmark, also known as a sweeping bookmark or a text fragment bookmark, can be used to show a larger expanse of text. This bookmark type is created by clicking and dragging text, hex, doc, or transcript content in the View pane.

## Notes Bookmarks

The notes bookmark gives the investigator a great deal of flexibility when adding comments to a report. This bookmark has a field reserved only for comment text and can hold up to 1000 characters. It also contains formatting options including:

- italics
- bold
- changing font size
- changing the indent of the text

## Folder Information/Structure Bookmarks

Use folder information bookmarks to bookmark folder structures or devices. By bookmarking a folder structure, the entire directory structure of that folder and its children can be shown within the report or bookmarked for later analysis. Individual devices, volumes, and physical disks can be bookmarked as well. This shows important device-specific information in the final report.

---

Note: This type of bookmark is useful for marking directories that contain unauthorized documents, pictures, and applications. It is also a great way to show specific information about the type of media in the case.

---

## Notable File Bookmarks

Use notable file bookmarks to bookmark individual files. These bookmarks provide a means of focusing the investigator's attention on specific files.

## File Group Bookmarks

File group bookmarks annotate a collection of individual files selected as a group. Bookmarking a collection of files helps the investigator organize evidence.

## Snapshot Bookmarks

Snapshot bookmarks include a wide variety of volatile data resulting from running the various EnScript® programs.

In EnCase® Forensic, the Scan Local Machine program creates snapshot bookmarks.

The output of the program is always bookmarked. After Scan Local Machine is run, a bookmark toolbar displays that contains the Home tab and the Snapshot tab. The Snapshot tab has a toolbar associated with it. This toolbar displays a tab command for each type of snapshot bookmark created by one of the EnScript programs.

Each type of snapshot bookmark has a Tree pane and Table pane associated with it. Each table displays data specific to the class of the system component whose data displayed in the Table pane.

Snapshot bookmarks include

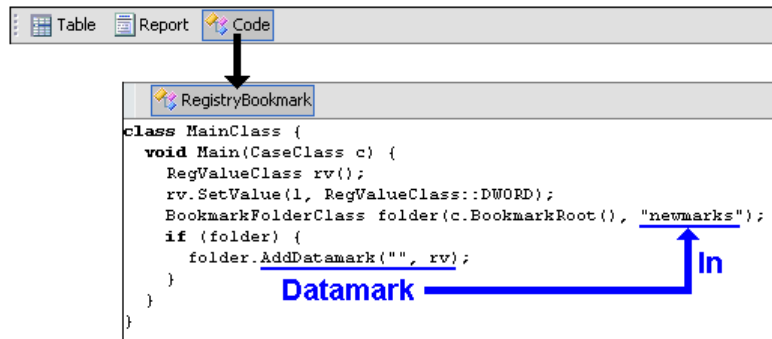
- Machines snapshot on the Home tab
- Open ports
- Processes
- Open files
- Network interfaces
- Network users
- DLLs

## Log Record Bookmarks

These bookmarks are created whenever console and status dialog messages are sent to a log record. Acquiring a device is one process that optionally sends its outputs to a log record, which results in a log record bookmark.

## Datamarks

EnScript programs or EnScript modules that execute the Add Datamark method create a datamark. When a datamark is created in a bookmark folder, that datamark can be used as a bookmark. Each datamark has a tab associated with it. The tab displays when you select the datamark in the Bookmarks table on the Bookmarks tab of the Tree pane.



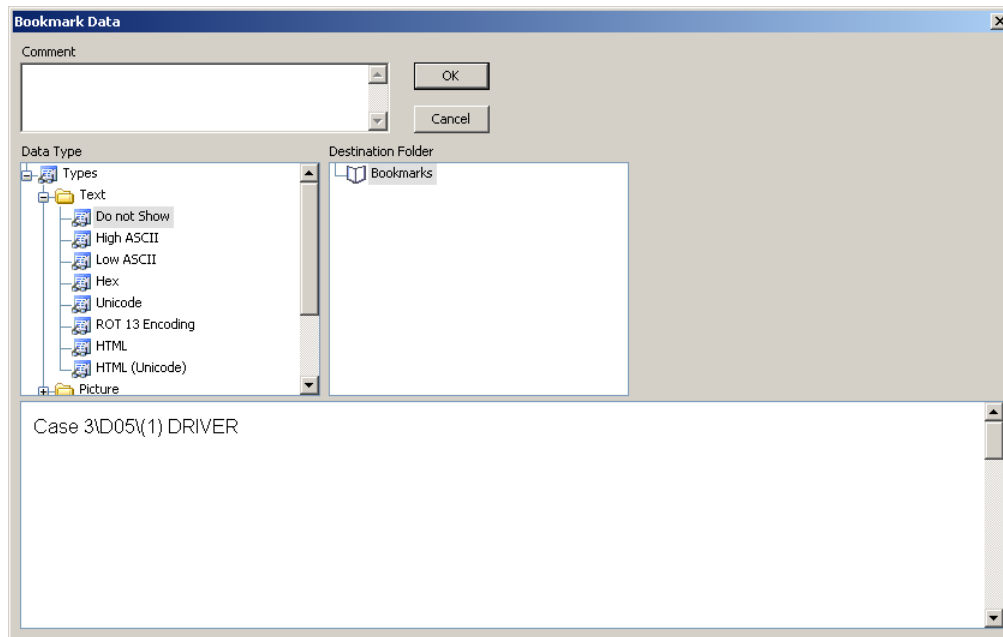
## Bookmark Features

Features that you use while working with bookmarks include:

- Bookmark Data dialog for highlighted data bookmarks
- Add Note Bookmark dialog
- Edit Folder Information/Structure Bookmarks dialog
- Bookmark Data dialog for files

## Bookmark Data Dialog for Highlighted Data Bookmarks

The Bookmark Data dialog is used when manually creating a bookmark. The dialog provides the means to add comments to the bookmark, determine the data type of the bookmark, and to select a destination folder where the bookmark is to be stored.



**Comment** contains text that describes the book marked content.

**Data Type pane** determines the data type of the book marked content.

**Types tree** contains objects representing the various formatting that can be used when displaying book marked content.

---

Note: Details of the content of the tree is described in Bookmark Content Data Types.

---

**Destination Folder** determines the path to the folder where the bookmark is saved.

**Contents** displays the content of the bookmark in the format selected.

## Bookmark Content Data Types

The Types tree in the Bookmark Data dialog provides a list of supported data types. The data types are organized by parent objects representing each class of supported data types. Each specific data type is represented by a child object. The formats interpret the underlying content. The formats change the way that the data is bookmarked.

## Text

Text is a parent object that contains child objects representing the formatting that can be used when displaying bookmarked content as text.

**Do not Show** hides the content of the bookmark. This works for all underlying data types.

**High ASCII** displays the text in 256-bit ASCII.

**Low ASCII** displays the text in 128-bit ASCII.

**Hex** displays the text as hexadecimal digits, rather than characters.

**Unicode** displays the text in Unicode encoding.

**ROT 13 Encoding** decodes ROT 13 encoded text to ASCII text.

**HTML** renders HTML coded as it appears in a browser.

**HTML (Unicode)** renders the HTML coded as it appears in a browser using Unicode encoding.

## Picture

Picture is a parent object that contains child objects representing various file formats that can be used when displaying bookmarked content as a picture or graphic.

**Picture** displays the bookmarked content of the following file formats:

- JPG
- GIF
- EMF
- TIFF
- BMP
- AOL
- ART
- PSD

This is based on the file extension or the file signature of the file that contained the book marked content.

**Base64 Encoded Picture** displays the bookmarked content in Base64 (Unicode) format.

**UUE Encoded Picture** displays the bookmarked content in UUE format.

## Integers

Integers is a parent object that contains child objects representing integer encodings that can be used when displaying bookmarked content.

**8-bit** displays the bookmarked content as 8-bit integers.

**16-bit** displays the bookmarked content as 16-bit Little-Endian integers.

**16-bit Big Endian** displays the bookmarked content as 16-bit Big-Endian integers.

**32-bit** displays the bookmarked content as 32-bit Little-Endian integers.

**32-bit Big Endian** displays the bookmarked content as 32-bit Big-Endian integers.

**64-bit** displays the bookmarked content as 64-bit Little-Endian integers.

**64-bit Big Endian** displays the bookmarked content as 64-bit Big-Endian integers.

## Dates

A date is a parent object that contains the objects representing various file formats that can be used when displaying bookmarked content.

**DOS Date** displays a packed 16-bit value that specifies the month, day, year, and time of day an MS-DOS file was last written to.

**DOS Date (GMT)** displays a packed 16-bit value that specifies the time portion of the DOS Date as GMT time.

**UNIX Date** displays a Unix timestamp in seconds based on the standard Unix epoch of 01/01/1970 at 00:00:00 GMT.

**UNIX Text Date** displays a Unix timestamp in seconds as text based on the standard Unix epoch of 01/01/1970 at 00:00:00 GMT.

**HFS Plus Date** displays a numeric value on a Power Macintosh that specifies the month, day, year, and time when the file was last written to.

**Windows Date/Time** displays a numeric value on a Windows system that specifies the month, day, year, and time when the file was last written to.

**Lotus Date** displays a date from a Lotus Notes database file.

## Windows

Windows is a parent object that contains objects representing the various file interpretations that can be used when displaying bookmarked content.

**Partition Entry** displays the content of the bookmark as characters that conform to the header format of a Windows partition entry.

**DOS Directory Entry** displays the content of the bookmark as characters that conform to the format of a DOS directory entry.

**Win95 Info File Record** displays the content of the bookmark as characters that conform to the INFO data structure definition.

**Win2000 Info File Record** displays the content of the bookmark as characters that conform to the INFO2 data structure definition.

**GUID** displays the content of the bookmark as strings that conform to the Windows Globally Unique Identifier (GUID) format.

**SID** displays the content of the bookmark in the Security Identifier (SID) format.

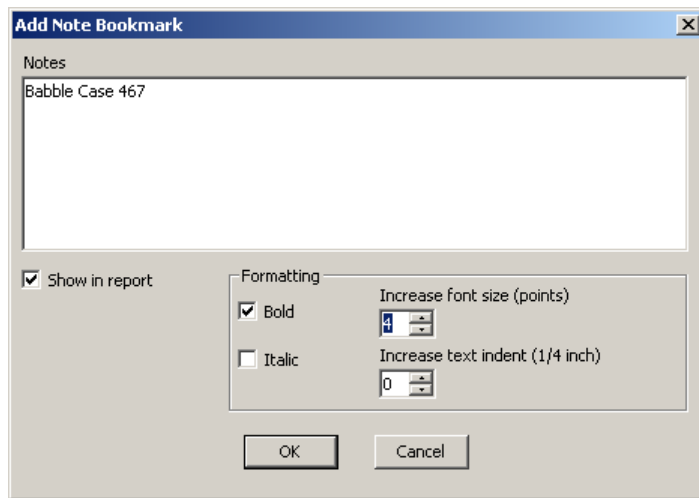
## Styles

Use these text styles when working with non-English languages. For more information see *Working with non-English Languages* (on page 457) elsewhere in this document.



## Add Note Bookmark Dialog

Use the Add Note Bookmark dialog to enter the note or text contained in a note bookmark. A note bookmark can contain up to 1000 characters. You can format the bookmark content as a whole. A note bookmark can annotate another existing bookmark, or add descriptions of events you want to include in a report.



**Notes** contains up to 1000 characters.

**Show in report** when checked, the content of the note bookmark appears in the Report tab of the Table pane.

**Formatting** contains the formatting controls for all characters that comprise the content of the note.

**Bold** makes all content of the note appear in bold.

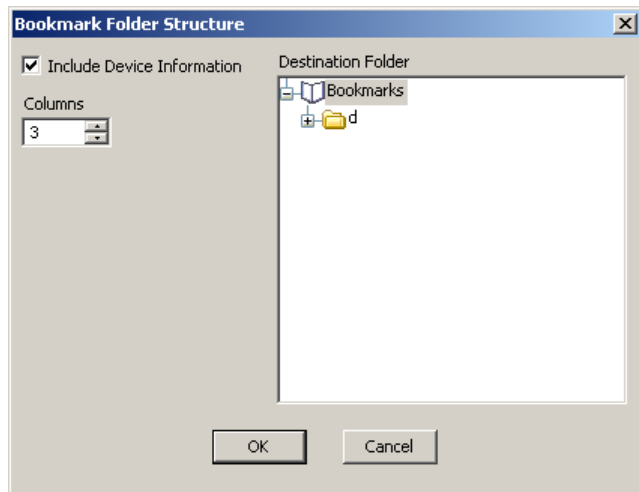
**Italic** makes all content of the note appear in italics.

**Increase font size** sets the font size of all the content of the note.

**Increase text indent** sets the text indent of all of the text blocks in the note.

## Bookmark Folder Information/Structure Dialog

Use the Bookmark Folder Structure dialog to determine whether and how much device information to include in the folder structure bookmark you are creating.

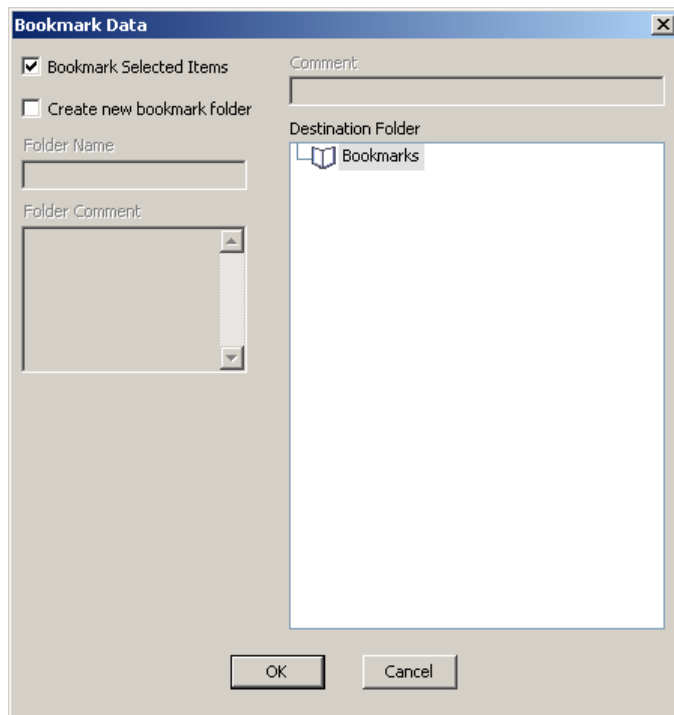


- **Include Device Information** includes folder structure information.
- **Columns** specifies the number of columns of folder structure information.
- **Destination Folder** displays the Bookmarks tree, so you can navigate to the destination folder.

## Bookmark Data Dialog for Files

Use the Bookmark Data dialog for files when creating notable files and file group bookmarks. The dialog lets you:

- add a short comment to the bookmark
- create a folder
- add a folder comment



**Bookmark Selected Items** appears when multiple files are selected on the Table pane. When checked, selected files are bookmarked as one or more file group bookmarks, and the Folder Comment field is disabled. When Bookmark Selected Items is cleared, only a single file was highlighted in the Table pane, and that single file is bookmarked as a notable file. Any other selected files are not bookmarked.

**Create new bookmark folder** determines whether a new folder is created, and whether **Folder Name** and **Folder Comment** are displayed.

**Folder Name** contains the filename for the new bookmark folder.

**Folder Comment** contains the comment describing the bookmarked files that the new folder contains.

**Comment** contains a short comment when using this dialog to create a notable file bookmark.

**Destination Folder** displays the Bookmarks tree so the destination folder can be selected.

## Creating a Bookmark

You can create these types of bookmarks:

- Highlighted Data
- Notes
- Folder Structure
- Notable File
- File Group
- Log Record

EnScript® programs create these types of bookmarks:

- Snapshot
- Datamarks

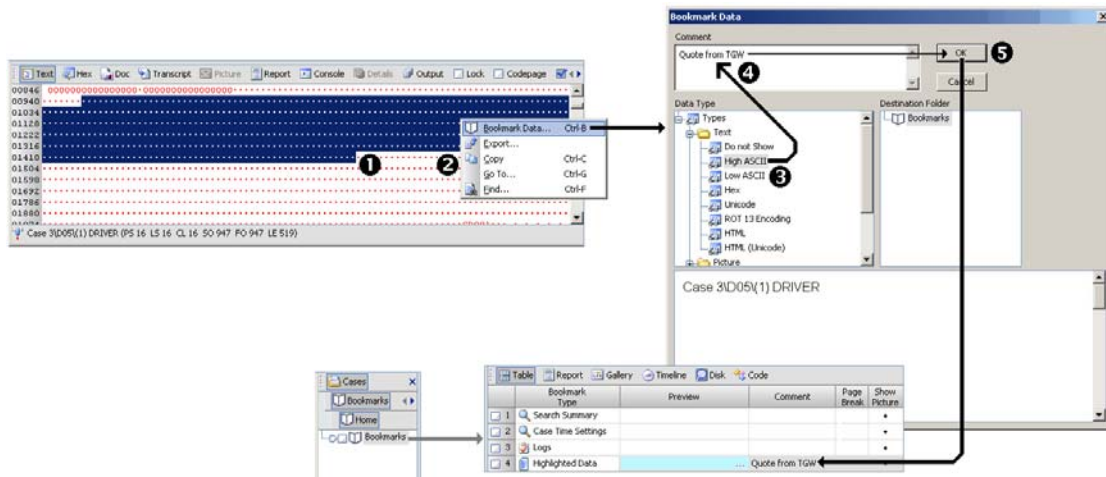
EnCase applications create these types of bookmarks as a result of acquiring a device:

- Case Time Settings
- Search Summary

## Creating a Highlighted Data Bookmark

You can select any content displayed in the View pane and bookmark it.

Content must display in a tab of the View pane.



*To bookmark highlighted content displayed in the View pane:*

1. In the View pane, select the desired content.
2. On the highlighted content, right-click **Bookmark Data**.  
The Bookmark Data dialog for highlighted data appears.
3. Select the appropriate data type in the **Types** tree.
4. Enter the desired comment.
5. Click **OK**.

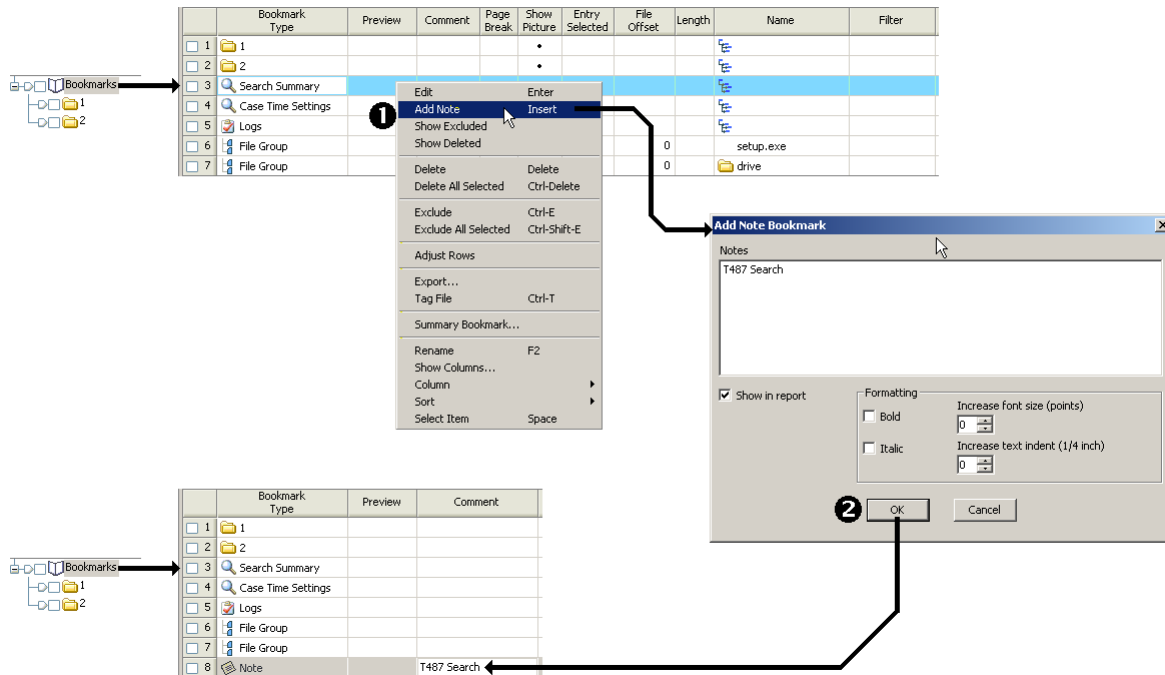
The comment appears in the **Comment** column of the Bookmarks table.

## Creating a Notes Bookmark

A note can contain up to 1000 characters. You can use a note to annotate a bookmark.

Before you begin:

- Create the desired bookmark
- Verify the bookmark it appears in the Bookmarks table in the Table pane



### To create a notes bookmark

1. In the Bookmarks table in the Table pane, right-click the desired bookmark, and click **Add Note**.

The Add Note Bookmark dialog appears.

2. Enter the text of the note, format the text as desired, and then change the **Appear in report** setting as desired
3. Click **OK**.

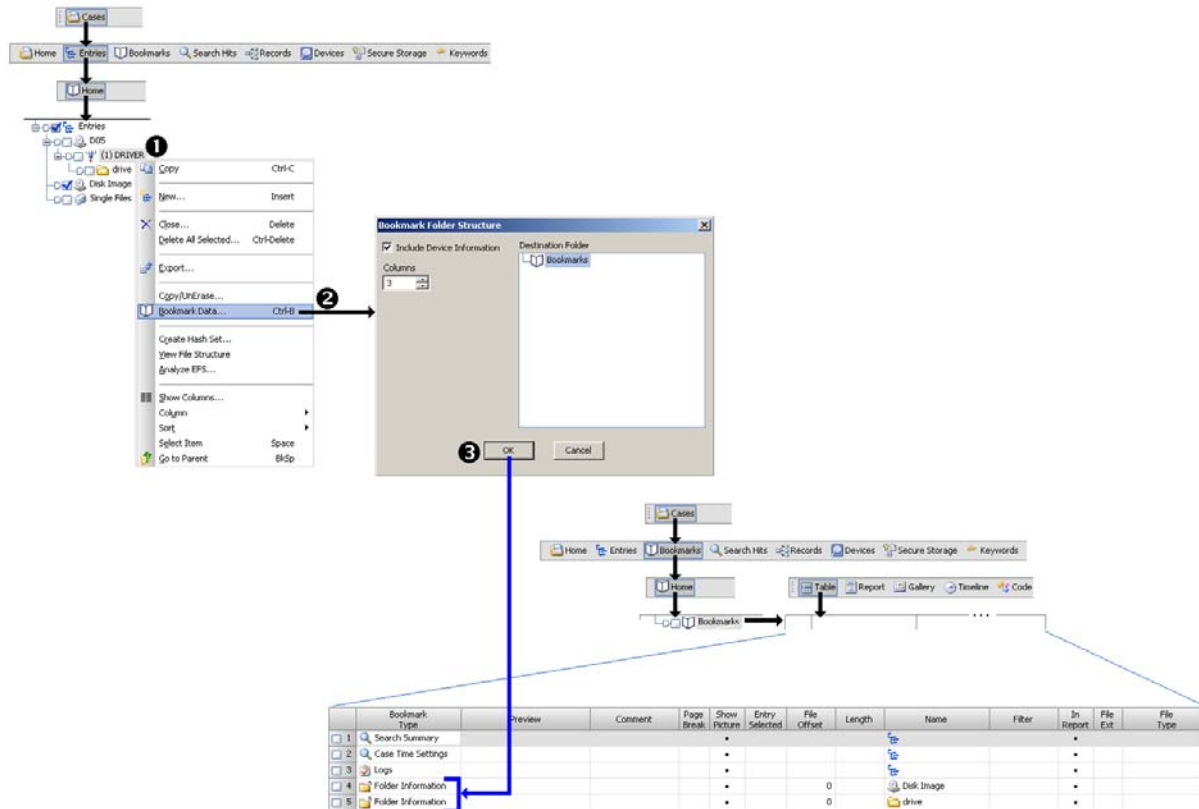
The note is added to the Bookmarks table on the Bookmarks panel in the Table pane.

## Creating a Folder Information/Structure Bookmark

Use a folder structure bookmark to bookmark a folder or device.

Before you begin:

The Entries tree must display in Entries panel of the Tree pane.



*To create a folder structure bookmark:*

1. Right-click the device or folder to bookmark, and click **Bookmark Data**.  
The Bookmark Folder Structure dialog appears.
2. Accept the default settings, or enter appropriate values.
3. Click **OK**.

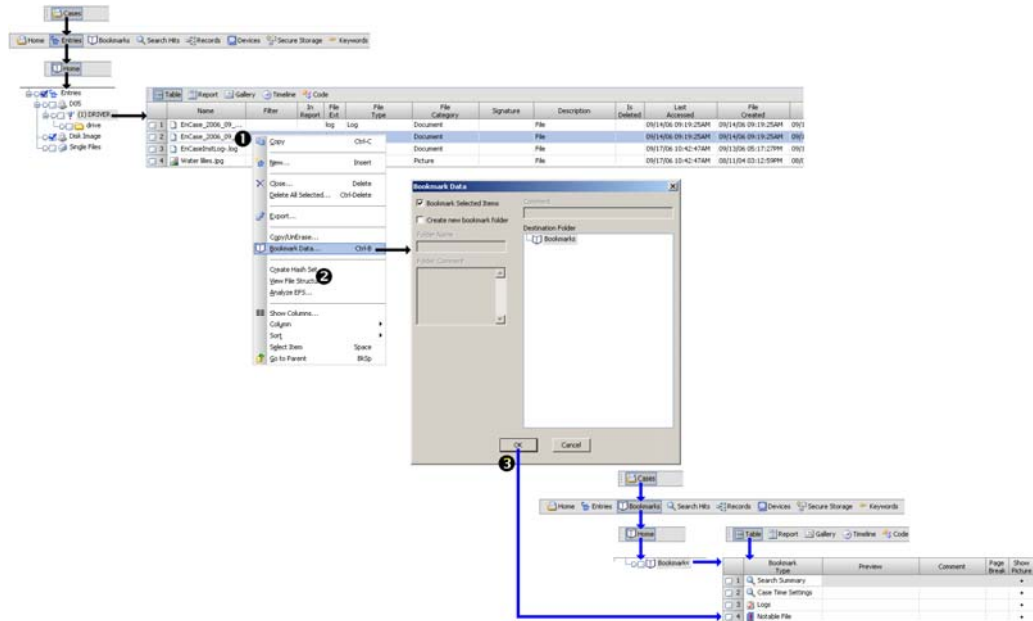
You can now view the folder structure bookmarks in the Bookmarks table of the Table pane.

## Creating a Notable File Bookmark

When you bookmark a single file, a notable file bookmark is created.

Before you can create a notable file bookmark, one of the following is required:

- The Entries tree must display in the Entries panel of the Tree pane.
- The Records tree must display in the Records panel of the Tree pane.



*To create a notable file bookmark:*

1. For the file to be bookmarked, select the device containing the file.
2. In either the Entries table on the Entries panel of the Table pane, or the Records table on the Records panel of the Table pane, select the row describing the file.
3. Right-click on the row describing the file.
4. Click **Bookmark Data**.  
The Bookmark Data dialog for files appears.
5. Accept the defaults or modify the values displayed on the Bookmark Data dialog
6. Click **OK**.

The notable file bookmark is placed in the Bookmarks table of the Table pane.

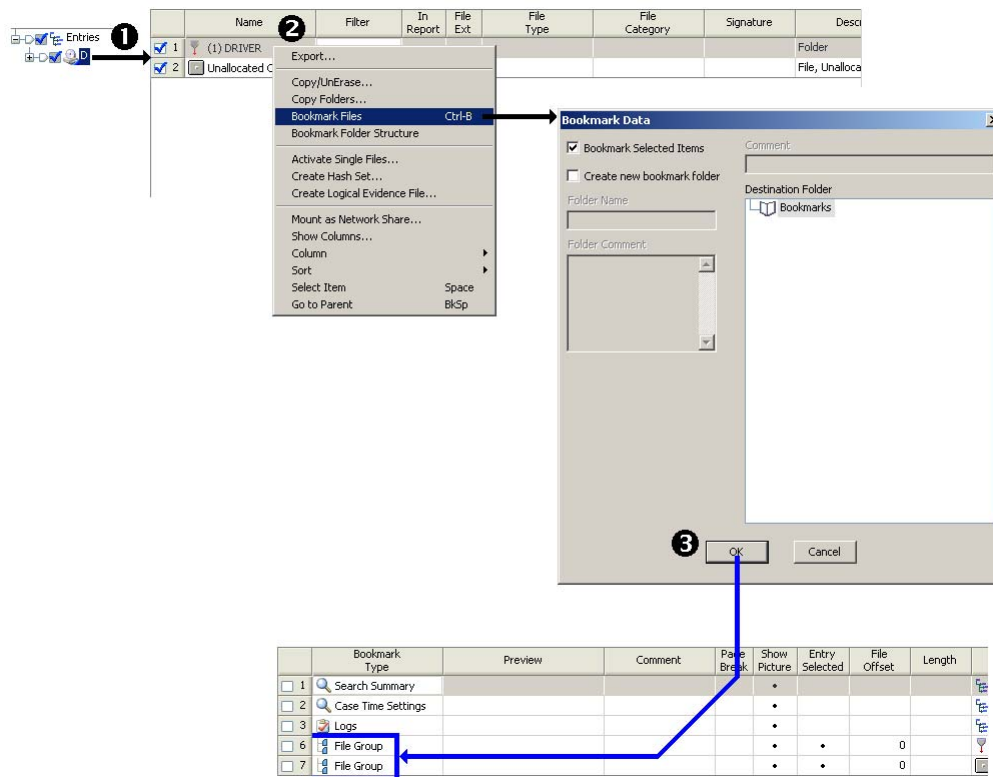


## Creating a File Group Bookmark

A file group bookmark is created if more than one file is selected in the Entries table.

Before you can create a file group bookmark, one of the following is required:

- The Entries tree must display in the Entries panel of the Tree pane.
- The Records tree must display in the Records panel of the Tree pane.



*To create group file bookmarks:*

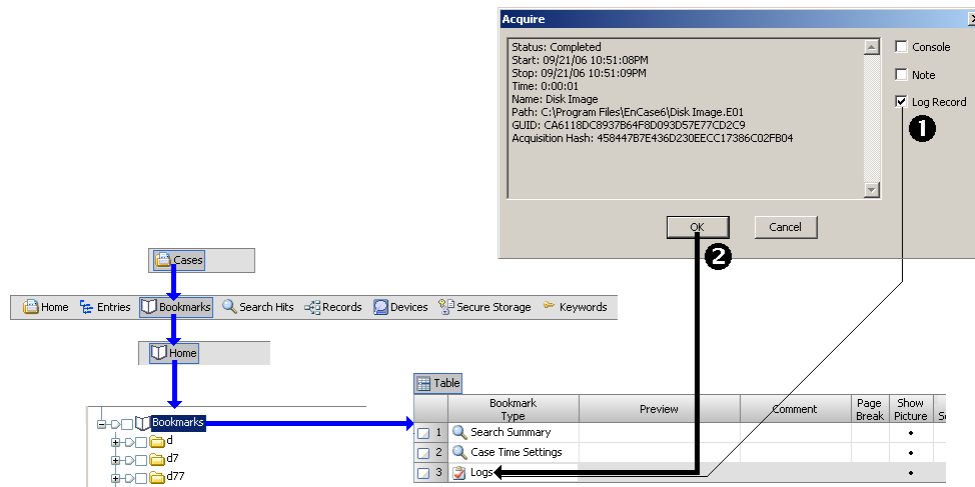
1. For the files to be bookmarked, highlight the device or parent folder containing the files.
2. In either the Entries table on the Table pane, or the Records table on the Table pane, select the files or to be bookmarked.
3. Click **Bookmark Data**.  
The Bookmark Data dialog for files appears.
4. Accept the defaults or modify the values displayed on the Bookmark Data dialog
5. Click **OK**.

The file group bookmarks are placed in the Bookmarks table of the Table pane.

## Creating a Log Record Bookmark

Log record bookmarks are created by a process status dialog (for example, the Acquisition Search Results dialog) that allows their content to be saved in a log record.

Before you can create a log record bookmark, a process results dialog must be open.



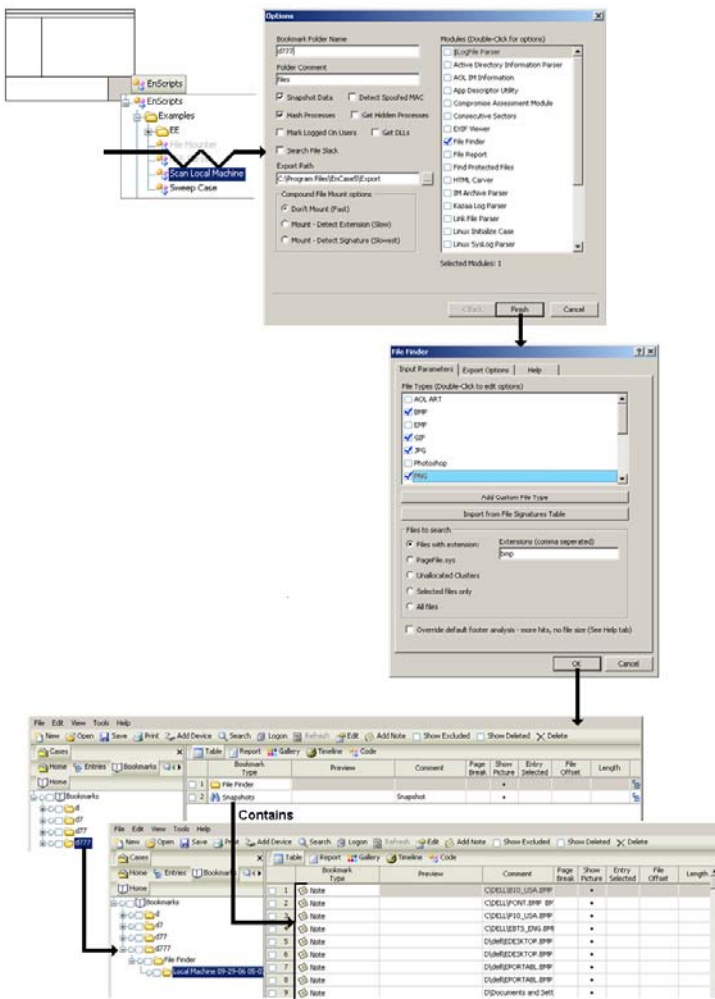
*To create a log record bookmark:*

1. On the process results dialog, select **Log Record**.
2. Click **OK**.

A Logs entry appears in the Bookmarks table in the Table pane.

## Creating a Snapshot Bookmark

Snapshot bookmarks are created by various EnScript programs. Note: Before you can create a snapshot bookmark, display the EnScript panel in the Filter pane.



*To create a snapshot bookmark:*

1. On the EnScript tree, expand the Forensic folder and double-click **Scan Local Machine**.  
The Options page of the EnScript wizard appears.
2. Enter a **Bookmark Folder Name**, select the desired modules, and click **Finish**.  
A dialog specific to the selected EnScript program appears.
3. Complete the EnScript program specific dialog, and click **OK**.

The Status Line shows the progress of the executing EnScript program. When the program finishes, the result appear in the Bookmarks display in the Tree pane and the Table pane.

4. See the resulting bookmarks by expanding the bookmark folder specified in step 2.

## Creating a Datamark as a Bookmark

EnScript programs can create datamarks and place them in any folder. When datamarks are placed in the Bookmark folder, they can be used to create a datamark and its associated tab panel containing data from the execution of the EnScript program.

To create a datamark as a bookmark, do one of the following:

- In the Code panel on the Table pane, right-click on the code, and click **Run**.
- In the EnScript panel of the Filters pane, expand the tree, and double-click the desired EnScript program object.

The EnScript program creates the datagram as a bookmark and creates a sub-tab named to match the name of the program that created it. In addition, an entry is output to the Output panel of the View pane.

## Using Bookmarks

You can create bookmarks on entries and records. These operations are available:

- Creating (see *Creating a Bookmark*) (see "Creating a Bookmark" on page 414)
- Editing (see *Editing Bookmarks*) (see "Editing a Bookmark" on page 423))
- Extending by adding a note bookmark (see *Creating a Notes Bookmark* (on page 416))
- Organizing into folders (see *Using Folders to Organize a Bookmark Report* (see "Using a Folder to Organize a Bookmarks Report" on page 431))

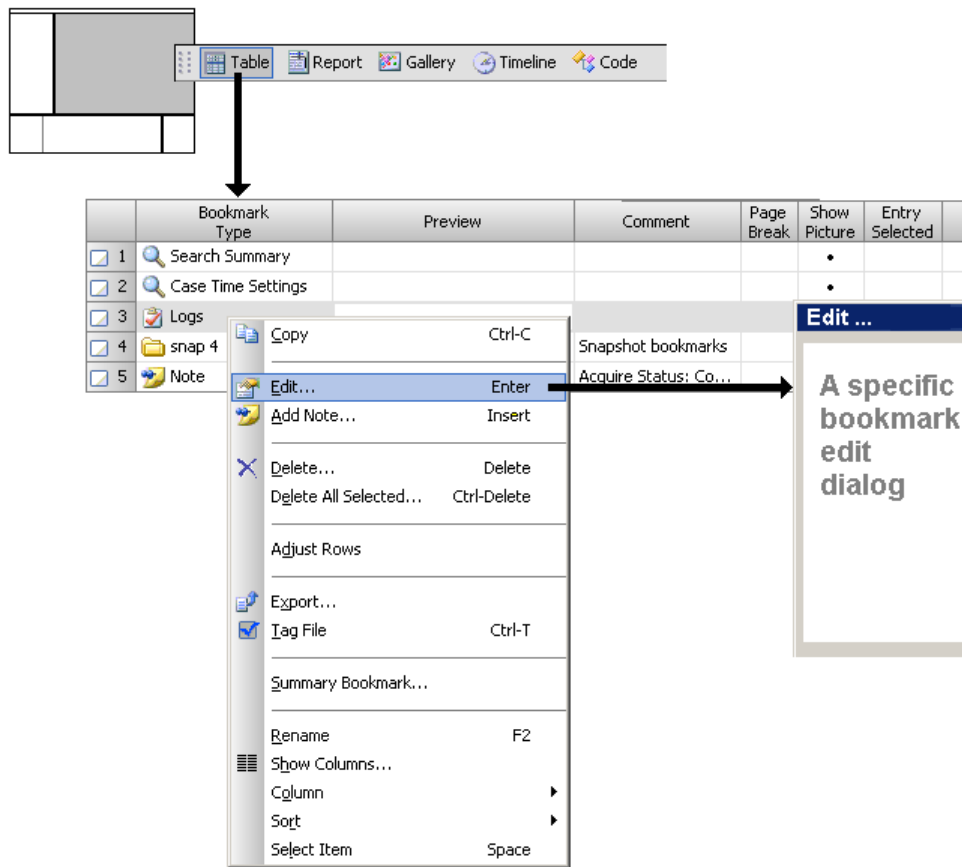
Reports can contain bookmarks and fields containing bookmark attributes:

- To determine which table entries should appear in a report, see *Viewing a Bookmark on the Table Report Tab* (on page 436).
- To determine which entry fields that should appear in a report, see *Customizing a Report* (on page 437).

## Editing a Bookmark

You can edit most bookmarks. The particular editor displayed is determined by the type of bookmark you are editing. See the individual edit dialogs for bookmark-specific information. The instructions in this topic apply to editing any bookmark except file group bookmarks, which cannot be edited.

**Note:** The contents of the Bookmarks table is driven by the object selected in the Tree pane.



*To edit a bookmark:*

1. In the Bookmark panel in the Table pane, right-click the desired bookmark, and click **Edit**.

The appropriate edit dialog appears.

2. Edit the content in the edit dialog
3. Click **OK**.

## Bookmark Editing Dialogs

These dialogs let you edit existing information entered when the bookmarks were created. However, for bookmarks that were created automatically, you can only enter or modify information once.

---

Note: File group bookmarks cannot be edited.

---

These editors are not necessarily the ones used to modify the data in the columns of the Bookmarks table on the Bookmarks panel of the Table pane.

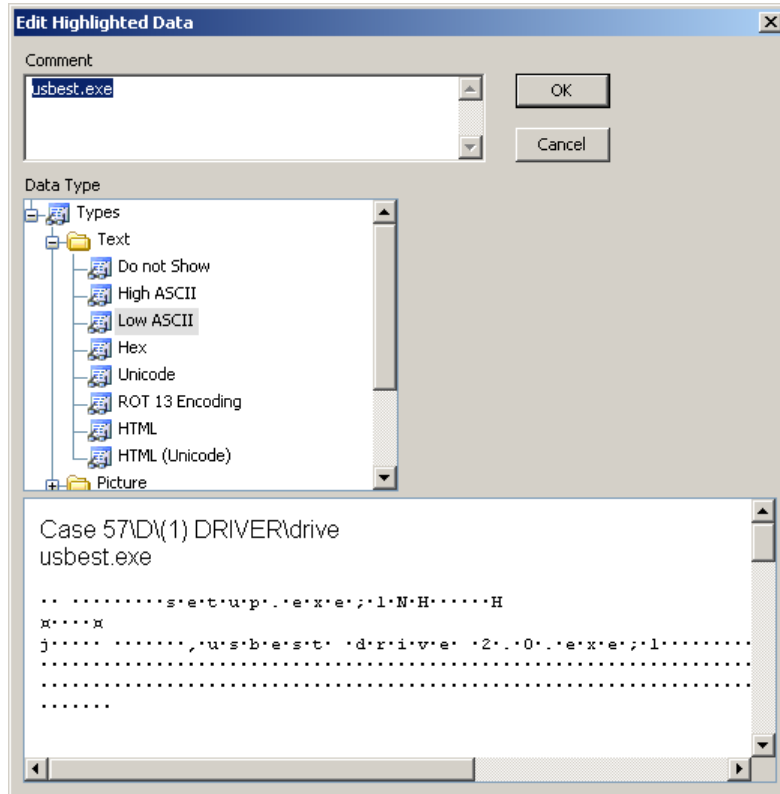
The bookmark edit dialogs include

- Edit Highlighted Data
- Edit Note
- Edit Folder Information/Structure
- Edit Notable File
- Edit Snapshot
- Edit Log Record
- Edit Datamark

Folders containing bookmarks are edited with the Edit Folder Dialog.

## Edit Highlighted Data Bookmarks Dialog

Use this dialog to edit highlighted data bookmarks.



**Comment** contains text describing the bookmarked content.

**Data Type** contains the data type of the bookmarked content. Selecting a different data type does not alter the content of the bookmark.

**Content** contains highlighted data that was bookmarked.

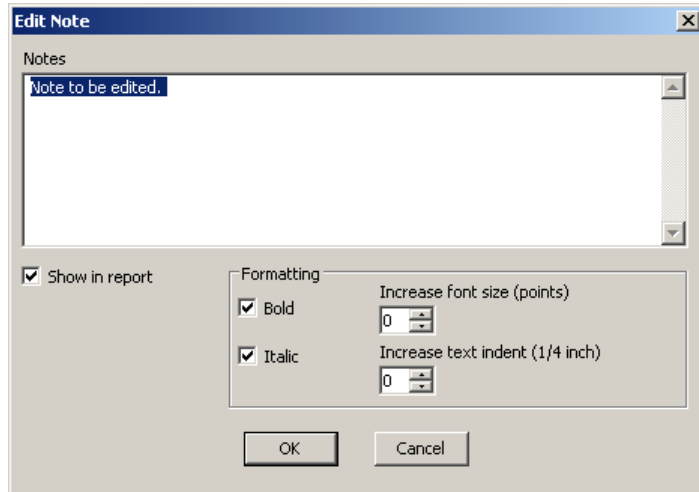
---

Note: You cannot edit this field.

---

## Edit Note Bookmarks Dialog

Use this dialog to edit notes bookmarks.



**Notes** contains text describing the bookmarked content. A note can contain up to 1000 characters.

**Show in report:** when checked, the content of the note bookmark appears in the report tab panel of the Table pane.

**Formatting** contains controls for formatting all characters in the note.

**Bold** makes all content bold.

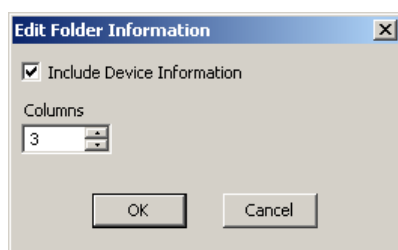
**Italic** makes all content italics.

**Increase font size** sets the font size of all content in the note.

**Increase text indent** sets the text indent of all of text blocks.

## Edit Folder Information/Structure Bookmarks Dialog

Use this dialog to edit folder information/structure bookmarks.



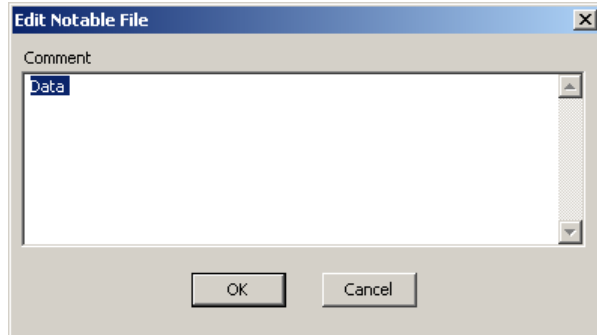


Check **Include Device Information** to show folder structure in the bookmark.

**Columns** determines the number of columns of folder structure to show in the bookmark.

## Edit Notable File Bookmarks Dialog

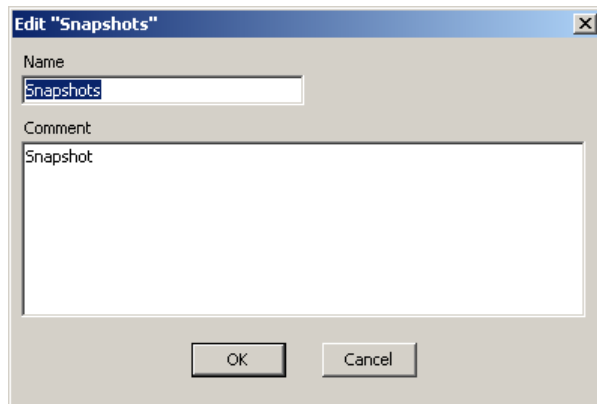
Use this dialog to edit notable file bookmarks.



**Comment** can contain up to 1000 characters.

## Edit Snapshot Bookmarks Dialog

Use this dialog to edit snapshot bookmarks.

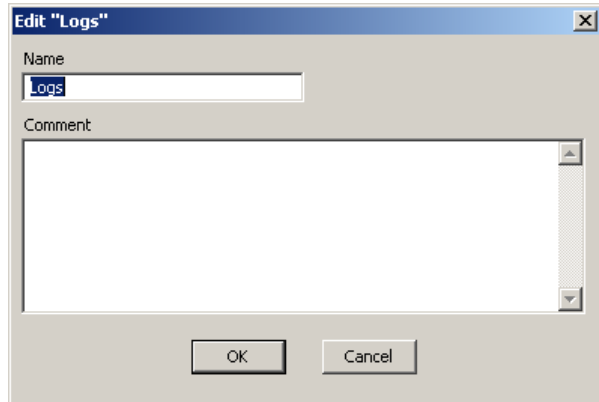


**Name** is the name of the snapshot bookmark. An EnScript® program supplied this name value when the bookmark was originally created. Editing lets you provide a more meaningful name.

**Comment** contains text describing the bookmarked content. An EnScript program supplied this text when the bookmark was originally created. Editing lets you provide more meaningful comments.

## Edit Log Record Bookmarks Dialog

Use this dialog to edit log record bookmarks.

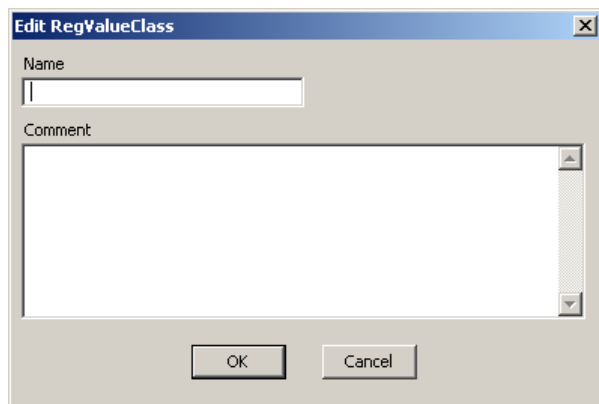


**Name** is the name of the log record bookmark. The EnCase® application supplied this name when the bookmark was originally created. Editing lets you provide a more meaningful name.

**Comment** contains text describing the bookmarked content. No text was supplied when the bookmark was originally created.

## Edit Datamarks Dialog

Use this dialog to edit datamarks as they appear as table entries. Datamarks can be used as bookmarks when they are created in the Bookmark folder.



**Name** is the name of the snapshot bookmark. The EnScript® program that created the datamark supplied this name when the datamark was originally created. Editing lets you provide a more meaningful name.

**Comment** contains text describing the bookmarked content. The EnScript program that created the datamark supplied this name value when the datamark was originally created. Editing lets you provide more meaningful comments.

## Edit Bookmark Folder Dialogs

Folders appear in the Bookmarks tree and the Bookmarks table. These folders contain metadata and formatting for the Report panels that appear in both the Table pane and the View pane.

---

Note: The root of the Bookmarks tree is a folder.

---

The same dialog (see Edit Folder Dialog) is used to edit the root bookmark folder and other folders in the Bookmarks tree and Bookmarks table. The root bookmark folder contains default report formatting while the other folders do not.

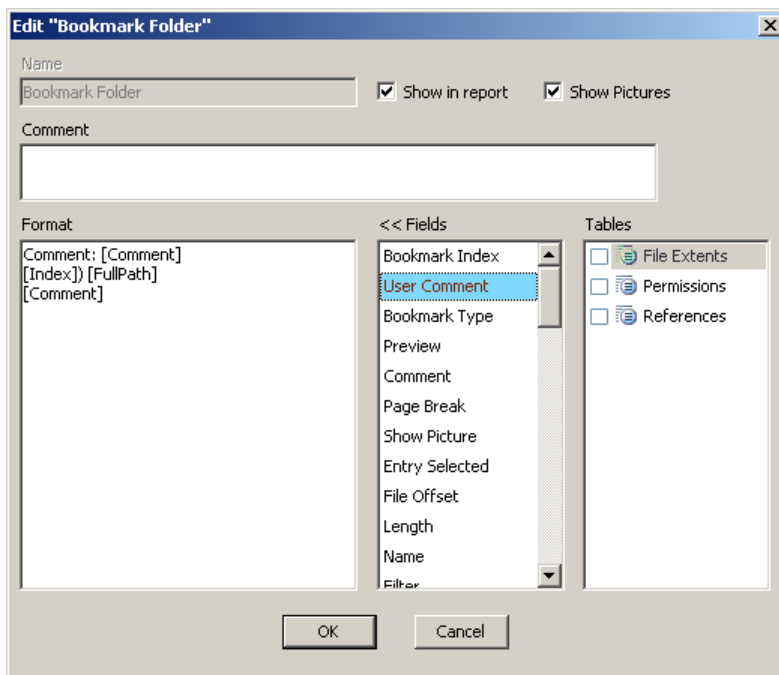
## Edit Folder Dialog

Use this dialog to modify:

- folder metadata
- report contents generated from the entries in the folder

This dialog works with any folder in any Tree or Table pane. When the folder is the root folder of a tree, default formatting is provided in the **Format** field.

You can also use this dialog to customize the report generated for the folder content. Each folder in a tree has its own report. Each folder defines its own report.



**Show in report:** check this box to display folder content in the report.

**Show Pictures:** check this box to display pictures in the folder in the report.

**Comment** contains text describing the bookmarked content.

**Format** contains labels (provided by the application or entered manually) and the fields selected in the Fields list. The label "Comment:" appears in the report. Square brackets contain a field. The ")" is a literal, as in another label. Everything other than fields are labels.

**Fields** contains the list of fields you can include in the report. This list varies from entry to entry.

**Tables** determines whether the listed detail tables display individually in the report.

# Using a Folder to Organize a Bookmarks Report

When several bookmarks are created, they appear in the bookmark report as selected by **In Report** in the Bookmarks table. Using folders is a way of selecting subsets of bookmarks to appear in the bookmarks report.

Before you begin:

- The Bookmarks tree displays in the Tree pane
- the destination folder is in the Bookmarks tree

The diagram illustrates the process of generating a bookmarks report using folders. It consists of several steps:

- Step 1:** The Bookmarks tree displays in the Tree pane. The tree shows a hierarchy starting with 'Cases' and 'Home'. Under 'Home', there is a 'Bookmarks' folder. This folder contains sub-folders 1, 2, 10, and 9. Folder 10 is highlighted.
- Step 2:** A 'Drag' arrow points from folder 10 to a table. This table lists various bookmark items with columns: Bookmark Type, Preview, Comment, Page Break, Show Picture, Entry Selected, File Offset, Length, Name, Filter, In Report, and File Ext.
- Step 3:** A second table shows the results of the drag operation. It lists items 1 and 2, both of type 'File Group'. Item 1 is 'setup.exe' and item 2 is 'usbest drive 2.0.exe'. Both have 'In Report' checked.
- Step 4:** A 'Drag' arrow points from the 'In Report' column of the second table to a third table. This table shows the final report output, which is a list of items with their full paths.
- Step 5:** The final report output is displayed in a window titled '2'. It shows a list of items with their full paths: '1) Case 1\DV(1) DRIVER\drive\setup.exe' and '2) Case 1\DV(1) DRIVER\drive\usbest drive 2.0.exe'.

To use folders to organize bookmarks:

1. Do one of the following:

To move a bookmark and remove it from the source bookmark object, drag the bookmark to the report in the destination folder.

To copy a bookmark from the source bookmark object, right-click and drag the bookmark to the destination folder, and select **Copy Here**.

The bookmark is now in the destination folder, so its entry now appears in the Bookmarks table associated with the destination folder.

2. Select the destination folder in the Bookmarks tree.

The bookmarks in the folder appear in the Bookmarks table.

3. In the Table pane, click **Report**.

The bookmarks in the folder appear in the report.

## Organizing Bookmarks

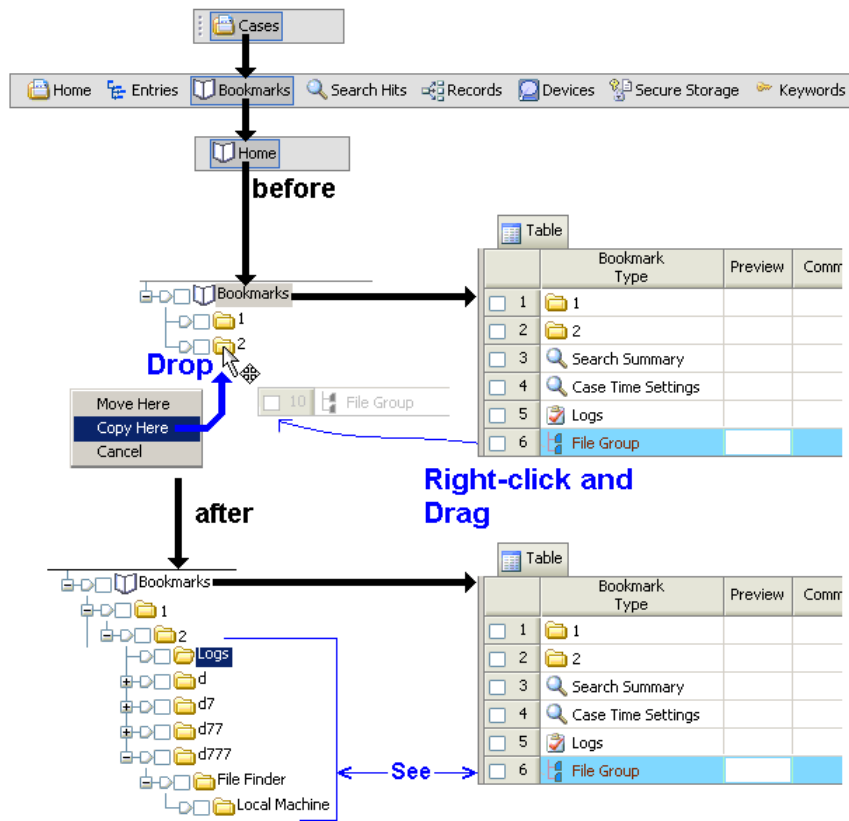
You can organize bookmarks into folders in the Tree pane. These folders appear in the Table pane, but a table entry cannot be dragged into other table entries. Instead, drag the table entry into a folder on the Bookmarks tree (see *Using a Folder to Organize a Bookmark Report* (see "Using a Folder to Organize a Bookmarks Report" on page 431)).

Organizing bookmarks involve the following tasks:

- *Copying a table entry into a folder* (on page 433)
- *Moving a table entry into a folder* (see "Moving a Table Entry into a Folder Using the Right-Click Drag Method" on page 434)

## Copying a Table Entry into a Folder

You can copy an entry in the Table pane to a folder in the Tree pane. Copying the entry leaves the entry in the table and creates a copy in the tree.

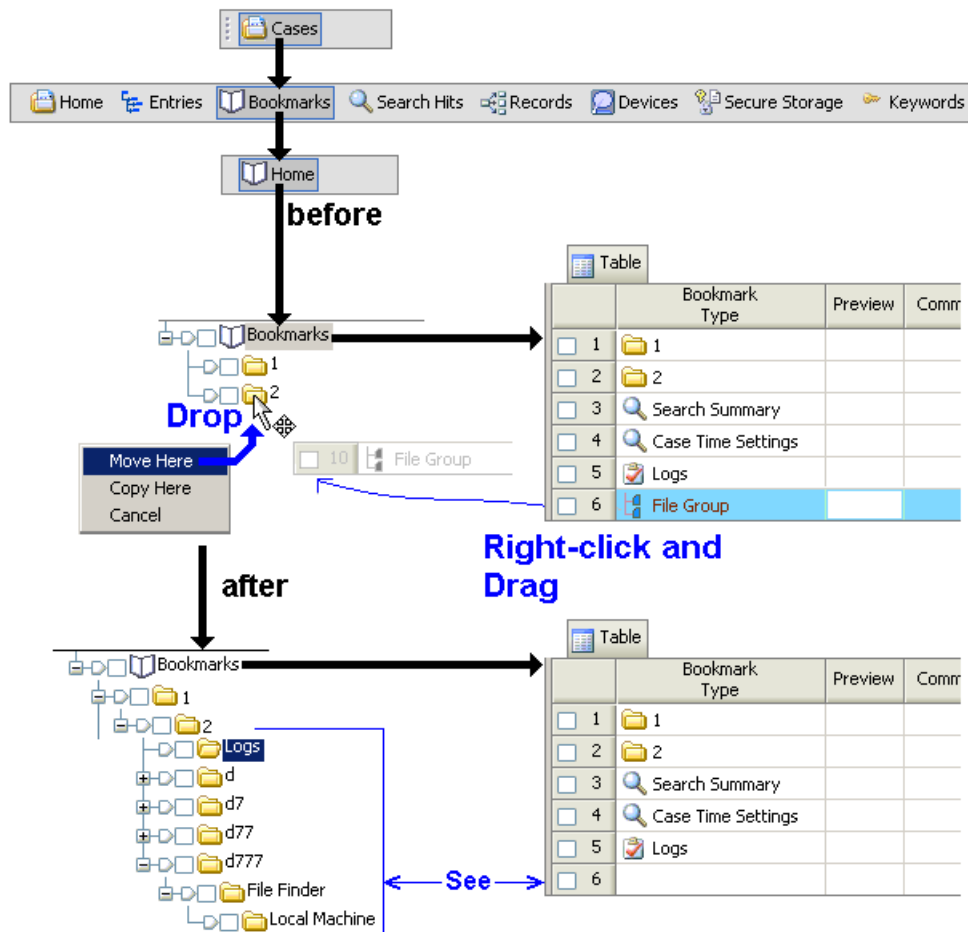


*To copy a table entry into a folder*

1. Right-click and drag the desired entry into the desired folder.
2. Drop the entry on the folder and select **Copy Here**.

## Moving a Table Entry into a Folder Using the Right-Click Drag Method

You can move a table entry into a folder using the right-click drag. The table entry is moved from the table to the tree.



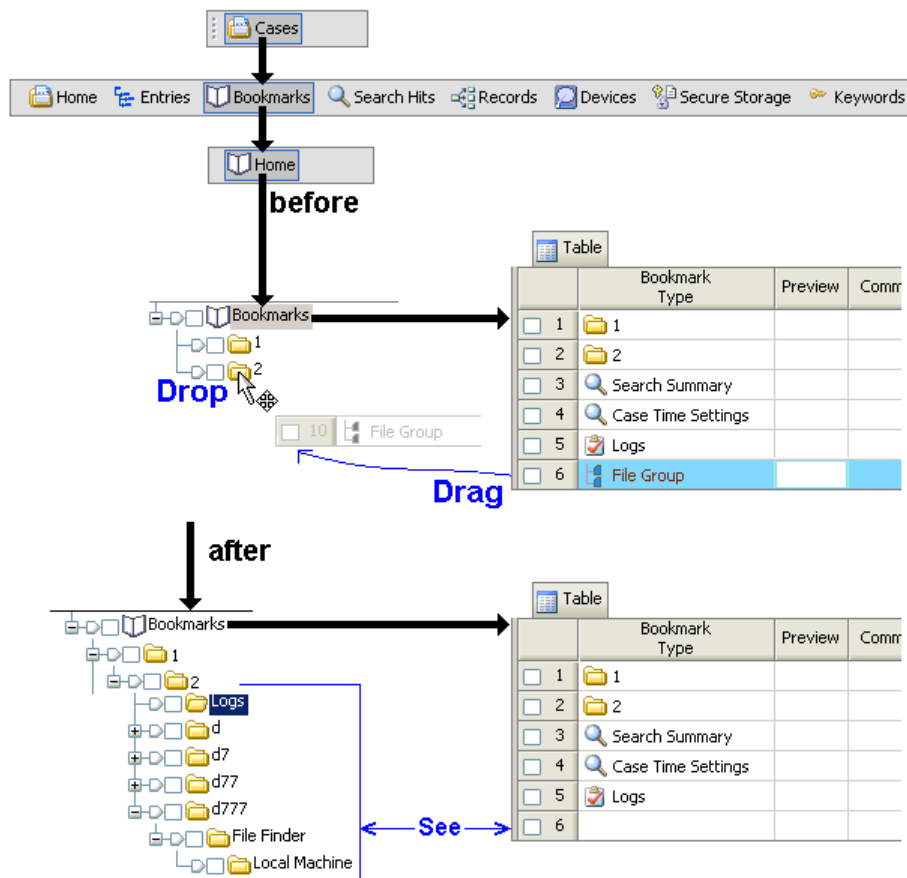
*To move a table entry into a folder using the right-click drag method*

1. Right-click and drag the desired entry into the desired folder.
2. Drop the entry on the folder and click **Move Here**.

The entry is moved to the folder on the tree and removed from the table.



## Moving a Table Entry or Folder into a Folder Using the Drag Method



1. Drag the desired entry or folder into the new parent folder.
2. Drop the entry or folder on the new parent folder.

The entry is moved to the folder on the tree and removed from the table.

## Bookmark Reports and Reporting

Bookmark reports content can be defined

- In the Table pane, as described in *View a Bookmark on the Table Report Pane* (see "Viewing a Bookmark on the Table Report Tab" on page 436) section.
- In the folder editor, as described in the *Customizing a Report* (on page 437) section.

## Viewing a Bookmark on the Table Report Tab

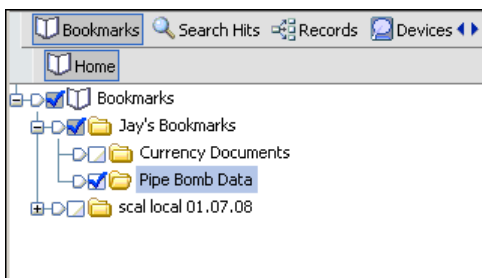
After you save a bookmark, it appears on the Report panel of the Table pane.

Before you begin:

Make sure the currently opened case has at least one bookmark associated with it. Click the **Bookmarks** tab and expand the view in the Table pane to display them.

*To view a bookmark report on the Report panel of the Table pane*

1. Select the bookmark folders you want to include in the report.

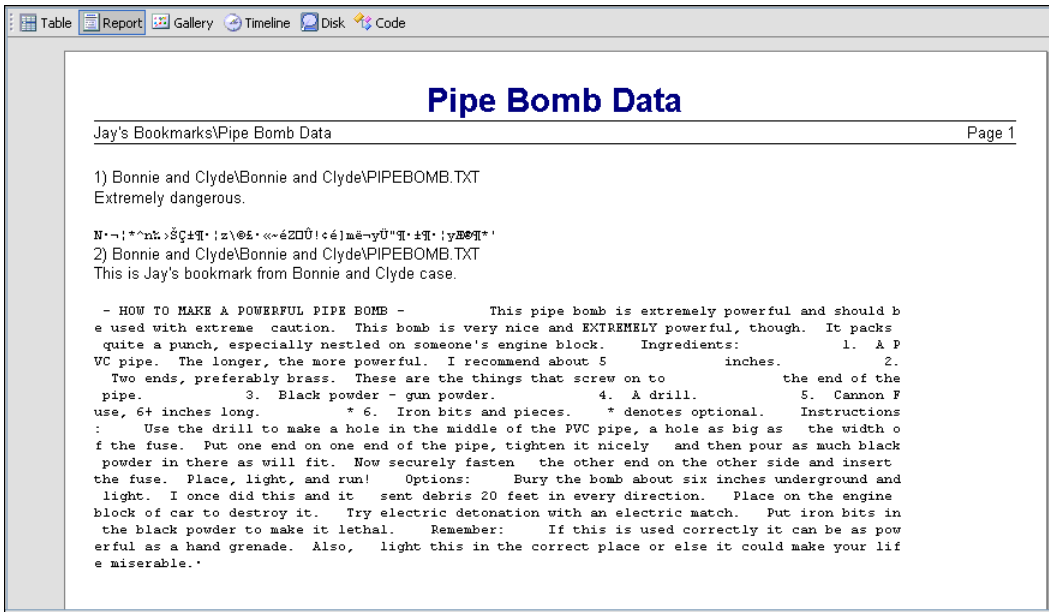


The folder contents appear checked in the Table pane. The first two data items are selected to be in the report, the third is not.

	Bookmark Type	Excluded	In Report
<input checked="" type="checkbox"/> 1	Highlighted Data	False	True
<input checked="" type="checkbox"/> 2	Highlighted Data	False	True
<input checked="" type="checkbox"/> 3	Note	False	False

2. To include a bookmark, make sure that the **In Report** column value for that bookmark is TRUE.

- On the Table pane toolbar, click **Report**. The report appears in the Report panel of the Table pane.



Note: To set the in-report value for multiple items, select several in the table panel of the table pane, and then follow the sub-step in step 2.

The report containing the bookmarked content and the metadata about the bookmarks can now be viewed.

## Customizing a Report

You can customize a report using the Edit Bookmark Folder dialog.

Note: Any bookmarks that will appear in the report must be in the same folder in the Bookmarks tree.

*To customize a report:*

- Right-click the folder containing entries for the report.
- Select **Edit**.  
The edit folder dialog appears.
- Using the **Fields** list, double-click each field in the order you want it to appear in the report.  
Each field is moved to the **Format** list.
- Enter any label text needed. The text appears in the **Format** list.
- Cut and paste the text and fields as needed. Once the content of the **Format** list is correct, click **OK**.

- On the Table pane, click **Report**.

The report appears with its customized contents.

## Excluding Bookmarks

Hiding all or parts of the listing is called **Excluding**. You can exclude any number of bookmarks from the Tree and the Table pane display using the **Exclude Bookmarks** feature.

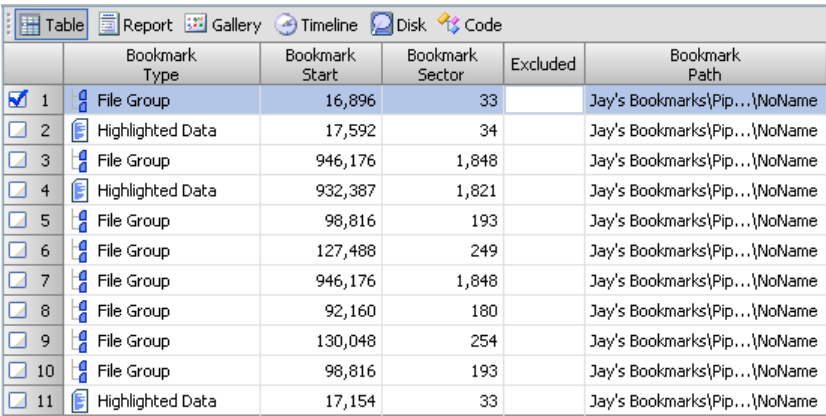
### Exclude File Bookmarks

In Bookmarks view, the Tree pane displays the bookmark folders you have created for an open case. You can prevent individual bookmark files from being displayed in the Table pane using the **Exclude Bookmarks** feature.

Before running this option, bookmarks must have been created in the open case.

*Exclude an entire folder of bookmarks as follows:*

- Open the bookmarks folder to view its contents.
- Select (blue-click or highlight) a file. The illustration below shows a graphic file checked.



	Bookmark Type	Bookmark Start	Bookmark Sector	Excluded	Bookmark Path
<input checked="" type="checkbox"/> 1	File Group	16,896	33		Jay's Bookmarks\Pip...\NoName
<input type="checkbox"/> 2	Highlighted Data	17,592	34		Jay's Bookmarks\Pip...\NoName
<input type="checkbox"/> 3	File Group	946,176	1,848		Jay's Bookmarks\Pip...\NoName
<input type="checkbox"/> 4	Highlighted Data	932,387	1,821		Jay's Bookmarks\Pip...\NoName
<input type="checkbox"/> 5	File Group	98,816	193		Jay's Bookmarks\Pip...\NoName
<input type="checkbox"/> 6	File Group	127,488	249		Jay's Bookmarks\Pip...\NoName
<input type="checkbox"/> 7	File Group	946,176	1,848		Jay's Bookmarks\Pip...\NoName
<input type="checkbox"/> 8	File Group	92,160	180		Jay's Bookmarks\Pip...\NoName
<input type="checkbox"/> 9	File Group	130,048	254		Jay's Bookmarks\Pip...\NoName
<input type="checkbox"/> 10	File Group	98,816	193		Jay's Bookmarks\Pip...\NoName
<input type="checkbox"/> 11	Highlighted Data	17,154	33		Jay's Bookmarks\Pip...\NoName

- Right-Click or press CTRL-E, then select **Exclude** from the menu.

The display reappears, but the selected file is not displayed.

## Exclude Folder

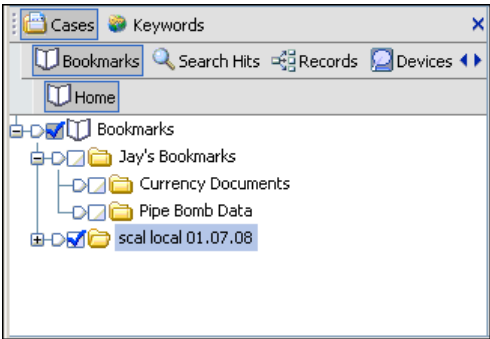
In Bookmarks view, the Tree pane displays the bookmark folders you have created for an open case. You can prevent bookmarked folders from being displayed in the Table pane using the **Exclude Bookmarks** feature.

Before running this option, bookmarks must have been created in the open case.

*Exclude an entire folder of bookmarks as follows:*

1. Select (blue-check or highlight) a folder.

Contents of the folder (`scal local 01.07.08` in the illustration) appear checked in the Table pane.

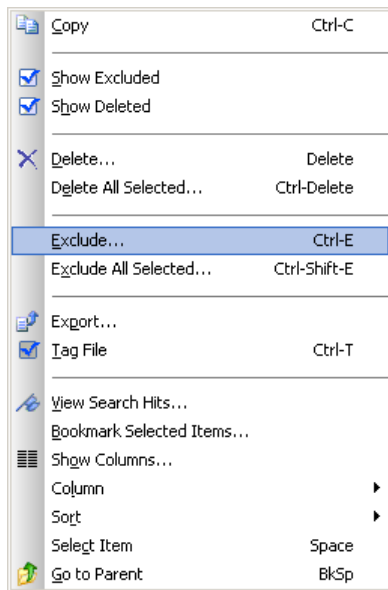


If you blue-check the folder, as shown in the illustration above, then open that folder, you'll see that the entire contents are selected, as below:

Table   Report   Gallery   Timeline   Code					
	Bookmark Type	Excluded	In Report	Notable	Comment
<input checked="" type="checkbox"/> 1	File Report				
<input checked="" type="checkbox"/> 2	HTML Carver				HTML Files with Keywords
<input checked="" type="checkbox"/> 3	Snapshots				Snapshot

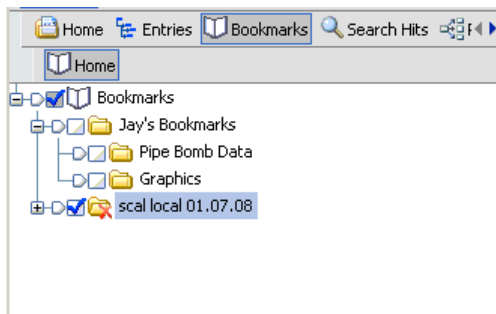
2. Right-click the folder you selected in the Tree pane.

A menu appears.



### 3. Select **Exclude**.

The Tree display reappears, but the excluded folder is marked with a red X.



The associated Table view is also marked as deleted.

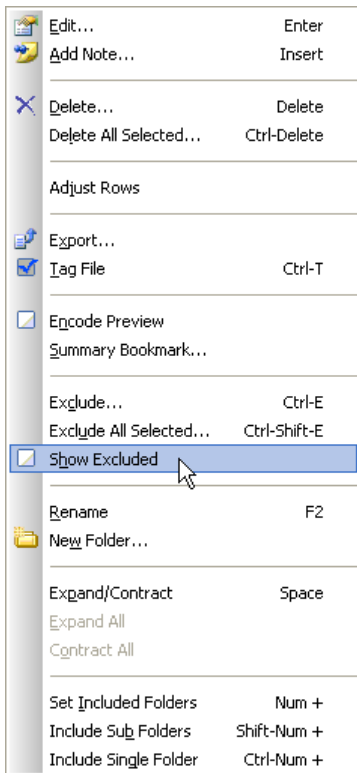
	Bookmark Type	Bookmark Start	Bookmark Sector
<input checked="" type="checkbox"/> 1	File Report		
<input checked="" type="checkbox"/> 2	HTML Carver		
<input checked="" type="checkbox"/> 3	Snapshots		
<input checked="" type="checkbox"/> 4	Highlighted Data	933,376	1,823

## Show Excluded

Excluded bookmarks are not deleted, they are merely hidden from view. It is possible to display them again if necessary.

You can show excluded files from the Tree pane, the Table pane from the Show Excluded too on the top toolbar. Regardless of the method you select, the steps are similar.

1. In the Tree pane, select and right-click a folder. This dropdown menu displays:



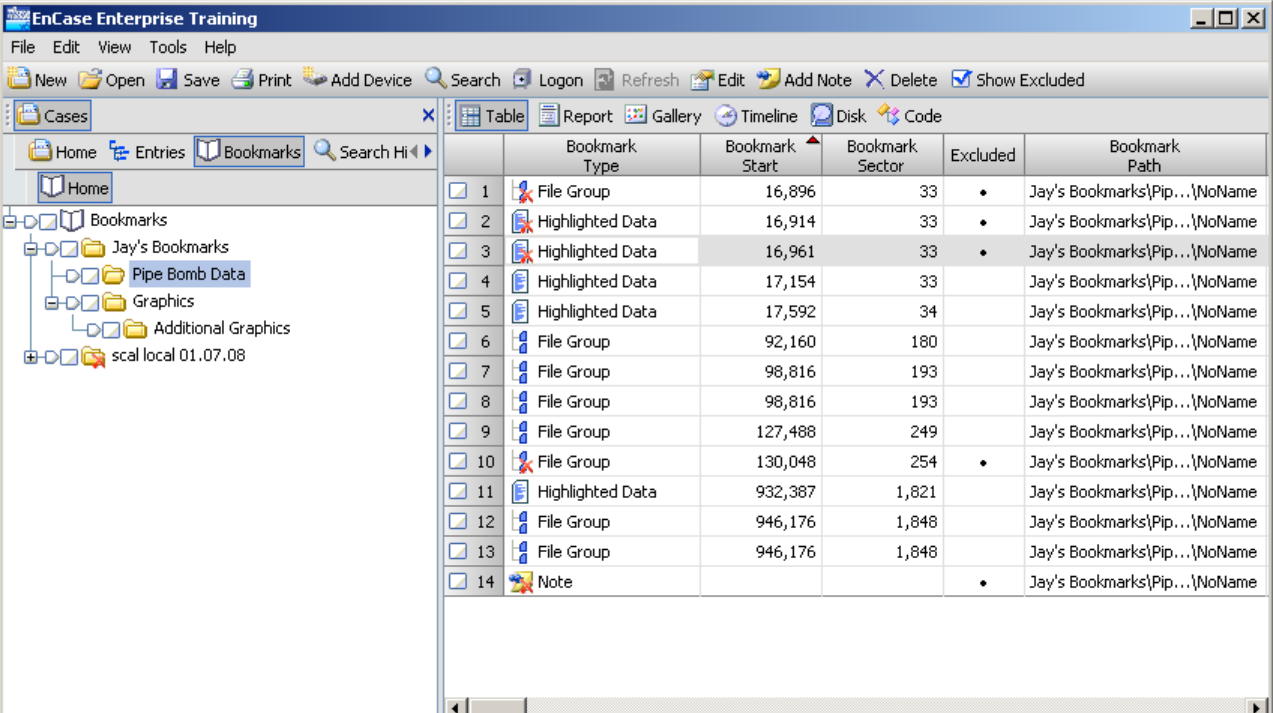
---

Note: In addition to the menu, there is a toolbar button labeled **Show Exclude** that toggles the hidden view.

---

2. Select **Show Excluded**.

Previously excluded files appear in Table view while exclude folders appear in the Tree view. Excluded data are marked with a red X.



	Bookmark Type	Bookmark Start	Bookmark Sector	Excluded	Bookmark Path
1	File Group	16,896	33	•	Jay's Bookmarks\Pip...\NoName
2	Highlighted Data	16,914	33	•	Jay's Bookmarks\Pip...\NoName
3	Highlighted Data	16,961	33	•	Jay's Bookmarks\Pip...\NoName
4	Highlighted Data	17,154	33		Jay's Bookmarks\Pip...\NoName
5	Highlighted Data	17,592	34		Jay's Bookmarks\Pip...\NoName
6	File Group	92,160	180		Jay's Bookmarks\Pip...\NoName
7	File Group	98,816	193		Jay's Bookmarks\Pip...\NoName
8	File Group	98,816	193		Jay's Bookmarks\Pip...\NoName
9	File Group	127,488	249		Jay's Bookmarks\Pip...\NoName
10	File Group	130,048	254	•	Jay's Bookmarks\Pip...\NoName
11	Highlighted Data	932,387	1,821		Jay's Bookmarks\Pip...\NoName
12	File Group	946,176	1,848		Jay's Bookmarks\Pip...\NoName
13	File Group	946,176	1,848		Jay's Bookmarks\Pip...\NoName
14	Note			•	Jay's Bookmarks\Pip...\NoName

Note: The **Excluded** column of the display shows which files are excluded and which are not.



# Reporting

- Reporting 443
- Creating a Report Using the Report Tab 444
- Creating a Report Using Case Processor 456

## Reporting

The final phase of a forensic examination is reporting findings. Organize and present reports in a way the target audience understands. Formatting and presentation considerations should be made when the evidence is first received. EnCase® software is designed to help mark and export findings so the final report is generated quickly.

The software provides several methods for generating a report. Some investigators prefer to break up the final report into several sub-reports in a word processing program, with a summary report directing the reader to the contents. Others create paperless reports on a compact disc, using a hyperlinked summary of the subreports and supporting documentation and files.

## Creating a Report Using the Report Tab

Creating reports is usually one of the last tasks performed when investigating a case. With the EnCase application, you can create reports based on data in any tab in the Tree pane.

Some of the most commonly created reports contain bookmarks or search hits.

Creating a report typically involves these steps:

1. Select the items to report on, whether files, bookmarks, search hits, or other data.
2. Select the type of report you want using the tabs in the Tree pane.
3. From the Table tab, in the View Pane, enable the items to show in the report.
4. From the Table tab, switch to the Report tab.
5. Modify the report as needed.
6. Export the report to a format viewable outside your EnCase application.

Examples of different types of reports are discussed in detail in later sections of this chapter.

## Enabling or Disabling Entries in the Report

Before entry data can be inserted in a formal report, they must be marked for inclusion.

	Name	File Ext	In Report	Description	File Type
<input type="checkbox"/> 13	bookmarks.htm	htm	No	File, Invalid Cluster, Arc...	Web Page
<input type="checkbox"/> 14	bookmarks.htm	htm	No	File, Invalid Cluster, Arc...	Web Page
<input type="checkbox"/> 15	bookmarks.html	html	Yes	File, Deleted, Overwritte...	Web Page

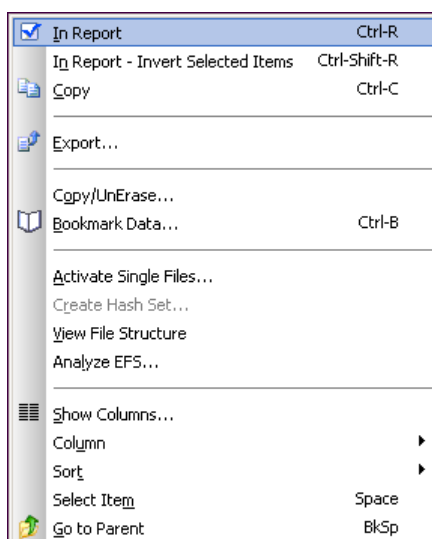
## Report Single Files

Open a case and display its contents in the Table pane.

1. Highlight the file to include in the report or check the box next to the record number (542 in the figure).

	Name	Filter	In Report	File Ext	File Type	File Category
<input type="checkbox"/> 539	MOG800B.BMP		Yes	BMP	Bitmap Image	Picture
<input type="checkbox"/> 540	MOG800X.BMP		Yes	BMP	Bitmap Image	Picture
<input type="checkbox"/> 541	PAG6106.BMP		No	BMP	Bitmap Image	Picture
<input type="checkbox"/> 542	MOG800BX.BMP		No	BMP	Bitmap Image	Picture
<input type="checkbox"/> 543	OKG700.BMP		No	BMP	Bitmap Image	Picture
<input type="checkbox"/> 544	MOG9000.BMP		Yes	BMP	Bitmap Image	Picture
<input type="checkbox"/> 545	8.BBS		No	BBS	Bulletin Board Text	Document
<input type="checkbox"/> 546	ATG1100.BMP		No	BMP	Bitmap Image	Picture
<input type="checkbox"/> 547	CLG1100.BMP		No	BMP	Bitmap Image	Picture

2. Place the cursor anywhere in the In Report column and right-click for a dropdown menu.



### 3. Select **In Report**.

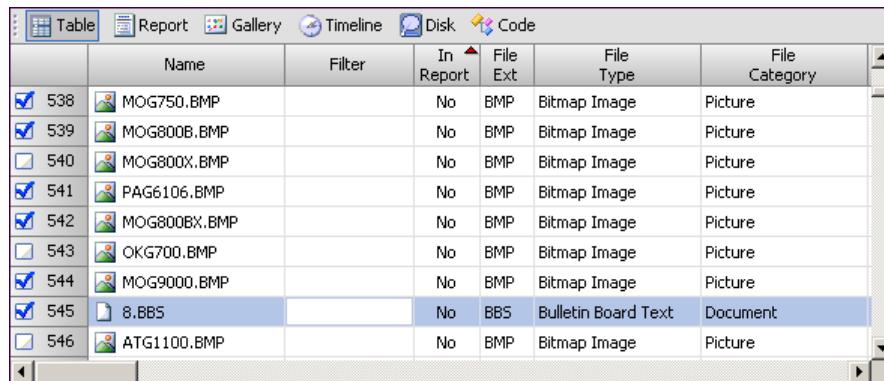
On the Table pane, the In Report column entry changes to a true value.

### 4. Click the Report panel to see its contents.

## Report Multiple Files

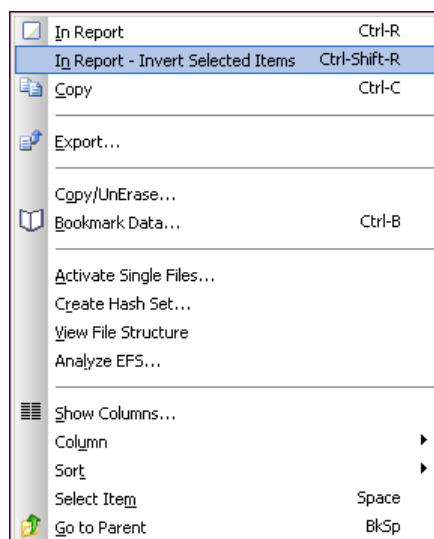
Open a case and display its contents in the Table pane.

1. Check the boxes next to the record numbers to include in the report (538, 539, 541, 544, and 545 in the figure).



	Name	Filter	In Report	File Ext	File Type	File Category
<input checked="" type="checkbox"/>	538	MOG750.BMP	No	BMP	Bitmap Image	Picture
<input checked="" type="checkbox"/>	539	MOG800B.BMP	No	BMP	Bitmap Image	Picture
<input type="checkbox"/>	540	MOG800X.BMP	No	BMP	Bitmap Image	Picture
<input checked="" type="checkbox"/>	541	PAG6106.BMP	No	BMP	Bitmap Image	Picture
<input checked="" type="checkbox"/>	542	MOG800BX.BMP	No	BMP	Bitmap Image	Picture
<input type="checkbox"/>	543	OKG700.BMP	No	BMP	Bitmap Image	Picture
<input checked="" type="checkbox"/>	544	MOG9000.BMP	No	BMP	Bitmap Image	Picture
<input checked="" type="checkbox"/>	545	8.BBS	No	BBS	Bulletin Board Text	Document
<input type="checkbox"/>	546	ATG1100.BMP	No	BMP	Bitmap Image	Picture

2. Place the cursor anywhere in the In Report column and right-click for a drop-down menu.

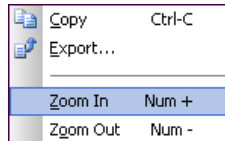


3. Select **In Report – Invert Selected Items**. In the Table view In Report column, the selected files change to True.
4. Click the Report tab to see its contents.

Note: This menu selection is an XOR switch. It changes the status of the In Report column to the opposite of what it was.

## Changing Report Size

To change the presentation size, right-click anywhere in the report display and select Zoom In or Zoom Out.

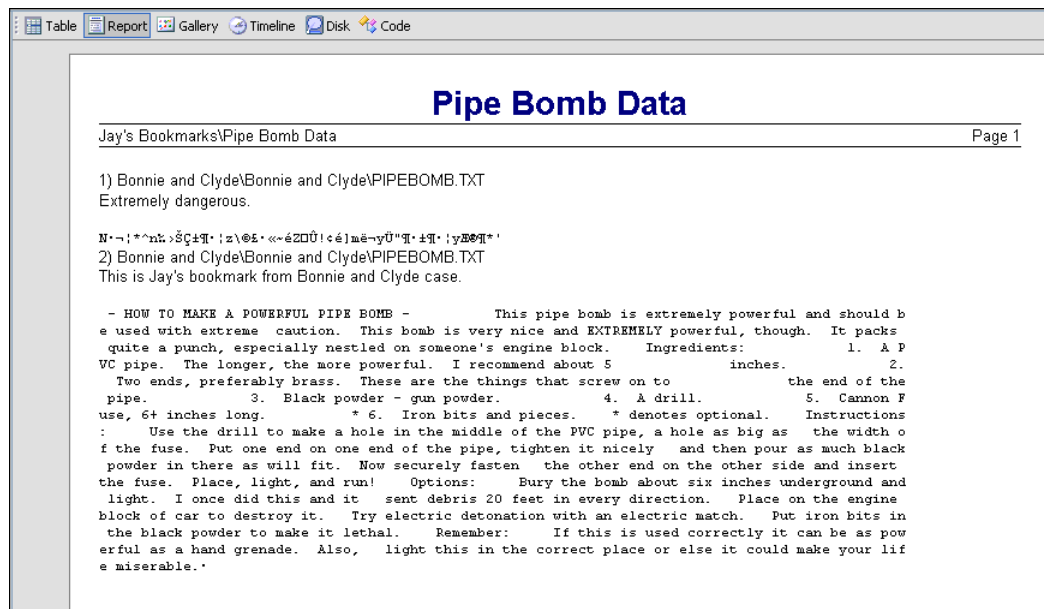


## Viewing a Bookmark Report

Open a case in the Table pane.

1. Click the Bookmarks panel.

The report appears.



The report is retained.

## Email Report

Email records are created when you perform an email search.

Perform an email search as described in the Creating a Report Using the Report Tab chapter.

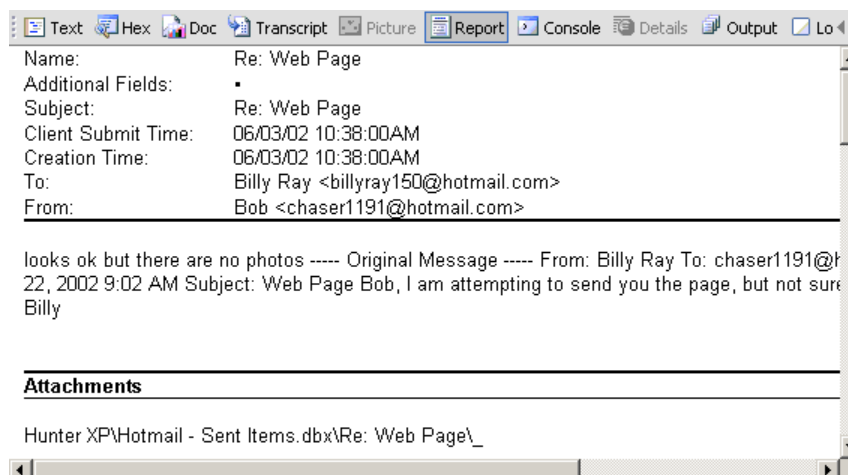
1. Select **View>Case Sub-Tabs> Records**.

A display of the Tree and Table panes appear. The Tree pane data show the records, and the Table pane displays the record's contents. The figure shows the contents of Hunter XP.

	Name	Filter	In Report	Search Hits	Additional Fields
<input type="checkbox"/> 1	Folders.dbx				
<input type="checkbox"/> 2	Billy.dbx				
<input type="checkbox"/> 3	chaser1191				
<input type="checkbox"/> 4	Hotmail - Sent Item...				
<input type="checkbox"/> 5	Outbox.dbx				
<input type="checkbox"/> 6	chaser1191				
<input type="checkbox"/> 7	Hotmail - Deleted It...				
<input type="checkbox"/> 8	Deleted Items.dbx				
<input type="checkbox"/> 9	3do.software.tools...				
<input type="checkbox"/> 10	Hotmail - Bank Infor...				
<input type="checkbox"/> 11	Bank Information.dbx				
<input type="checkbox"/> 12	Hotmail - Inbox.dbx				

2. Select a record from the Tree pane, then click the Report panel of the Report pane.

Selecting an entry from the Table pane displays an individual report like this:



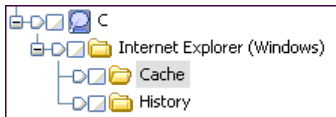
## Internet Report

Records for an Internet history report are created when you execute an Internet search.

Perform an email search as described in the Creating a Report Using the Report Tab chapter.

1. Select **View >Case Sub-Tabs > Records**.

The Tree and Table panes appear. The Tree pane data show the records, and the Table pane displays the record's contents. Note the subfolders, Cache and History.



2. Select either Cache or History to display their contents in the Table pane.
3. Select a record from the Tree pane, then click the Report panel of the Report pane.

The report displays in the Report pane.

## Creating a Webmail Report

Complete the Webmail Parser

1. Select the folder to see its contents in the Table pane.
2. Select a file to report on, then select the Report tab of the Report pane. The report displays.



## Alternative Report Method

You can generate a report in the Table pane as well.

1. Select the file in the Table pane.
2. Click the In Report column to include the item in the report.
3. Click the Report panel of the Table pane to view the report.





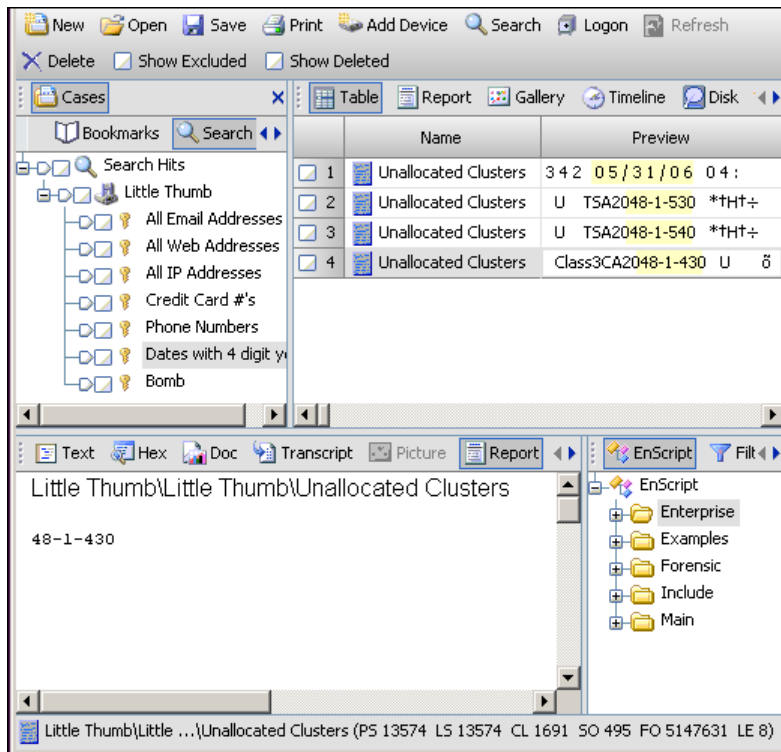
## Search Hits Report

Keyword searches require good reports. Sometimes found keywords are a significant part of a case. There are several permutations of keyword search reports.

Run a standard keyword search.

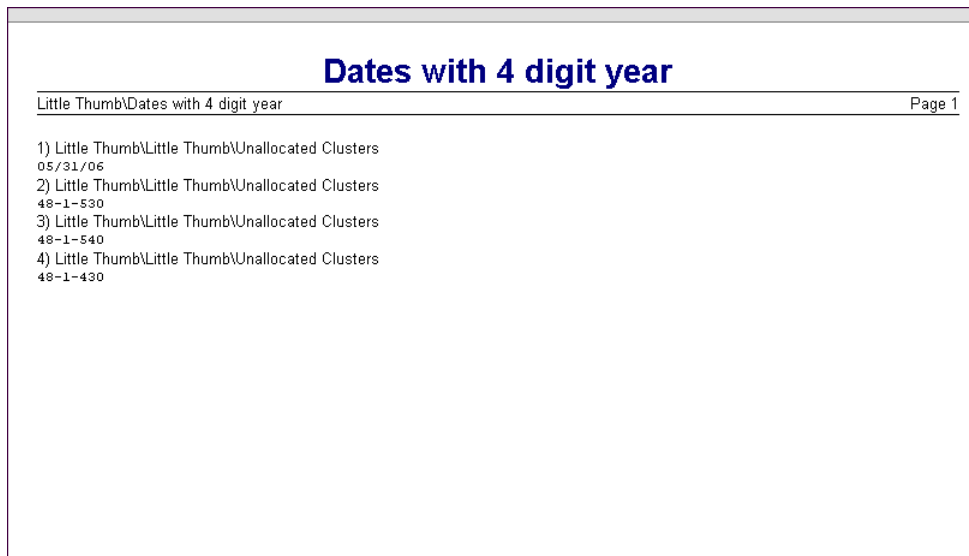
1. Click **Search Hits**.

The four-pane display shows results of the search.



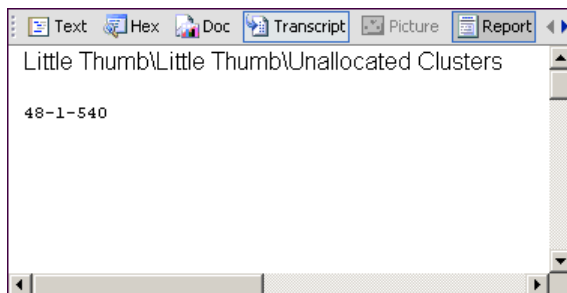
2. Select a keyword in the Table pane.
3. Click **Report**.

Results of the selected Table pane keyword appear in the Report pane.



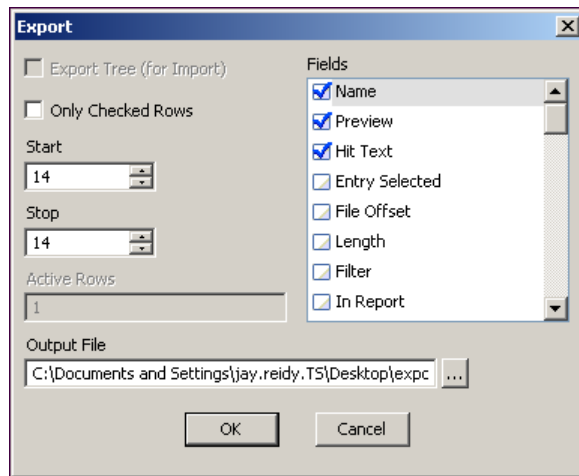
4. Select an item in the Table pane.

An report containing the file name, address, and the contents of the Tree pane keyword displays.



5. Right-click in the Table pane.
6. Complete the dialog and click **OK**.

Check the fields to display in the report and designate an output location and file name in the Output File field.



A delimited text file is created.

Save the reports in accordance with local policy.

## Quick Entry Report

Often, a quick report containing information regarding one particular file in a case is needed.

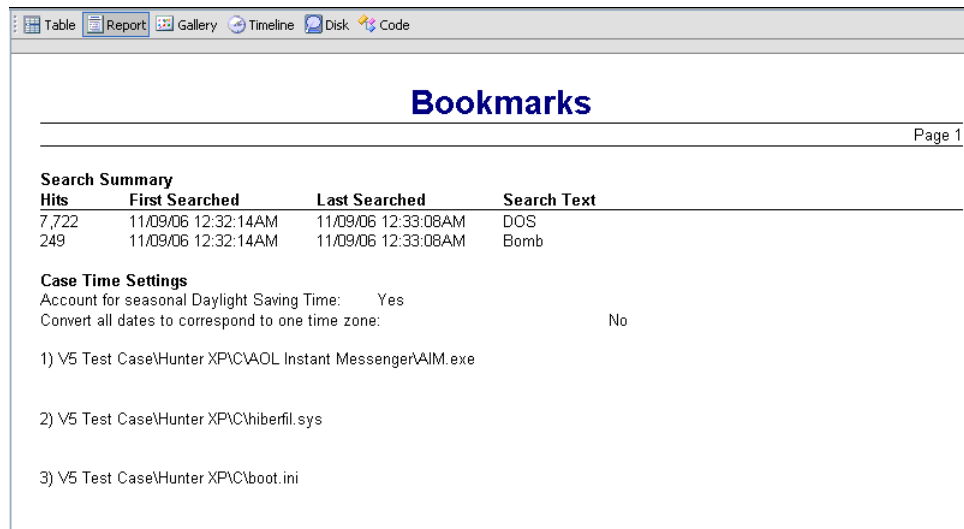
Start by opening a case that has bookmarked files, then locating the file you want to report on.

1. Select the file to use to generate a report.

	Name	File Ext	In Report	Description	File Type
<input checked="" type="checkbox"/> 13	bookmarks.htm	htm	No	File, Invalid Cluster, Arc...	Web Page
<input checked="" type="checkbox"/> 14	bookmarks.htm	htm	No	File, Invalid Cluster, Arc...	Web Page
<input checked="" type="checkbox"/> 15	bookmarks.html	html	Yes	File, Deleted, Overwritte...	Web Page

2. In the View pane, click **Report**.

A short report displays.



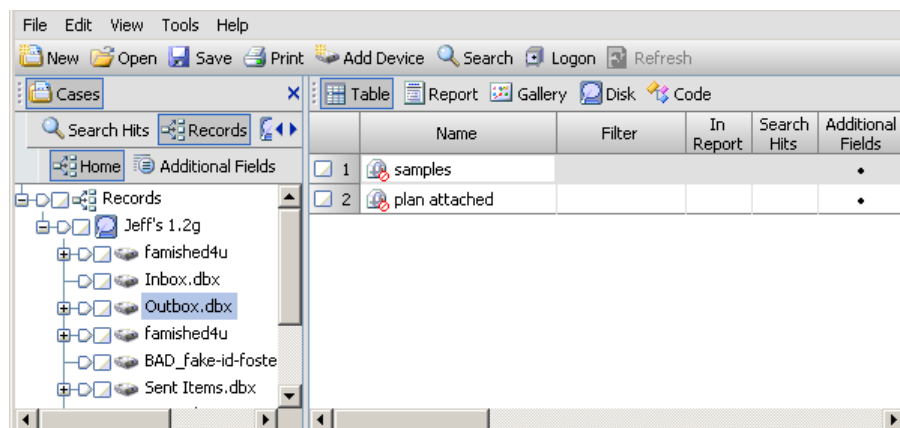
The report displays in the Report panel of the Table Pane.

## Creating an Additional Fields Report

The Additional Fields panel is available when you select the Records panel. Data in the additional fields varies depending on the type of data contained in the record. Your EnCase application is open, and you have a case created with evidence in it.

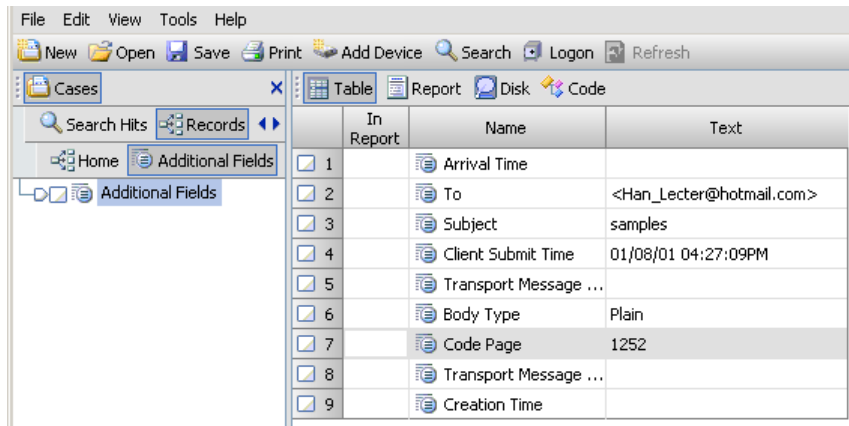
Open a case containing evidence.

1. Click the **Records** panel to make the Additional Fields panel available.



2. In the Table pane, select the entry where you want to view additional fields.
3. Click the **Additional Fields** panel in the Tree pane.

Note: Additional fields are only available on entries showing a true value in the Additional Fields column in the Table Pane.



4. If the In Report column is not shown, enable it:
  - a. Right-click in the Table pane and select **Show Columns**.
  - b. Select In Report and click **OK**.

The In Report column appears in the Table panel.

5. Select the fields you want to include in the report. See *Enabling or Disabling Entries in the Report* (on page 445).
6. Click the Report Panel in the View pane.

The report is generated containing the enabled fields.

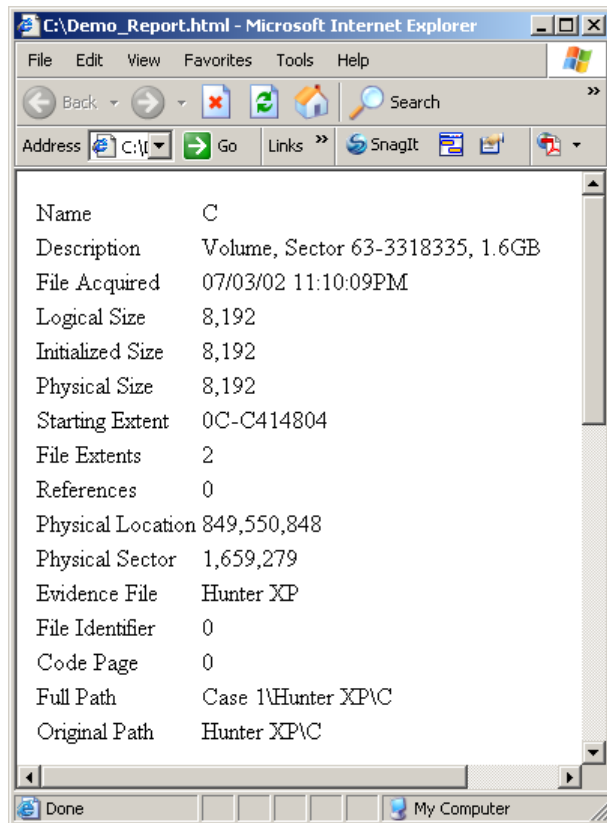
## Exporting a Report

Once a report is generated, you can save it to a file.

*Place the cursor in the report.*

1. Right-click and click **Export**.  
The Export Report dialog appears asking for output information.
2. Select the appropriate output format.
3. Enter or navigate to the desired output path.  
The newly created report document is saved to a file.

Here's a web page generated from the Export routine.



## Creating a Report Using Case Processor

You can create reports using the Case Processor EnScript program.

The Case Processor Report Generator contains these features:

- Entry Attributes such as File Group, Notable Files, Highlighted Data, Folder Info, Email information, and Records.
- Ability to report on only items tagged In Report.
- Ability to report on only selected items in the Records tab.
- The report captures the investigator's name, organization name and creation date.
- The report is generated as HTML, viewable outside of EnCase. The data is organized like the Table tab, and breaks down each set of information by its evidence file.

# Working with Non-English Languages

- Working with Non-English Languages 458
- Non-English Language Features 459
- The Options Dialog Font Tab 460
- Configuring Non-English Language Support 465

## Working with Non-English Languages

This chapter covers a specialized area of investigations: working with languages other than English.

The Unicode standard attempts to provide a unique encoding number for every character regardless of platform, computer program, or language. Unicode encompasses a number of encodings. In this document, Unicode refers to UTF-16 (Unicode 16-bit Transformation Format).

Currently more than 100 Unicode code pages are available. Because EnCase applications support Unicode, investigators can search for and display Unicode characters, and thus support more languages.

Other character codes besides 16-bit Unicode are supported for working with non-Unicode non-English-language text.

Working with non-English languages typically involves performing these tasks:

- Configuring non-English language support
- Creating and applying a new text style
- Creating non-English language search terms
- Bookmarking non-English language text
- Viewing Unicode files
- Viewing Non-Unicode files
- Using Code Pages in the Text and Hex tabs



## Non-English Language Features

EnCase Enterprise applications provide non-English language support through various features, including:

- The Options dialog Fonts tab
- Text styles

Use text styles to modify the display of content:

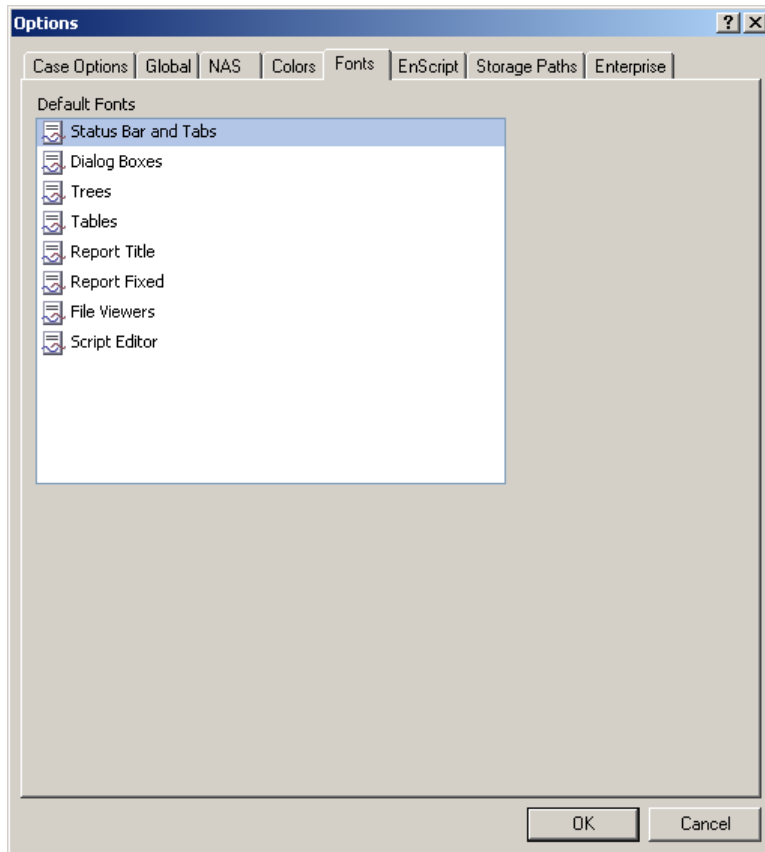
- The text pane
- The transcript pane

Text styles are defined globally on the Text Styles tab. When defined, these text styles are not associated with a case. In the Filter pane, you can:

- Create text styles
- Edit text styles
- Apply text styles to content in the View pane

## The Options Dialog Font Tab

This Options tab contains a list of EnCase interface elements that you configure to support non-English languages. Each of the listed elements has font settings associated with it. Double-clicking an element opens the Font dialog where you select the associated settings.



**Default Fonts** contains the list of interface elements to be configured. Double-clicking on these interface elements opens the Font dialog. Selecting a Unicode font enables non-English language text to display in these interface elements.

## Unicode Fonts

Specific fonts in the Fonts dialog are installed in Windows. If no Unicode fonts are installed on your computer, see Install the Universal Font for Unicode at <http://office.microsoft.com/en-us/help/HP052558401033.aspx> <http://office.microsoft.com/en-us/help/HP052558401033.aspx>.

Unicode interprets fonts as 16-bit words. When Unicode fonts are selected, 8-bit character sets and 7-bit ASCII characters do not display correctly. Use an 8-bit font such as Courier New for English text

To properly display the characters in certain code pages, you should only select a Unicode display font.

Characters that are not supported by the font or code page display as a default character, typically either a dot or a square. Modify this character when using text styles in the Text and Hex tabs of the View pane.

## Text Styles

The display of non-English language content is controlled by both the type face of the content, and the text style applied to the content. A text style applies various attributes to fonts, including:

- Line wrapping
- Line length
- Replacement character
- Reading direction
- Font color
- Class of encoding
- Specific encoding

Text styles are applied in the Text, Hex, and Transcript panes. See Viewing Non-Unicode Files, and Viewing Unicode Files for more information. You can create and edit text styles. See Creating and Defining a New Text Style for more information.

Text styles are global; therefore, they are not associated with a specific case, but rather can be applied to any case after they are defined.

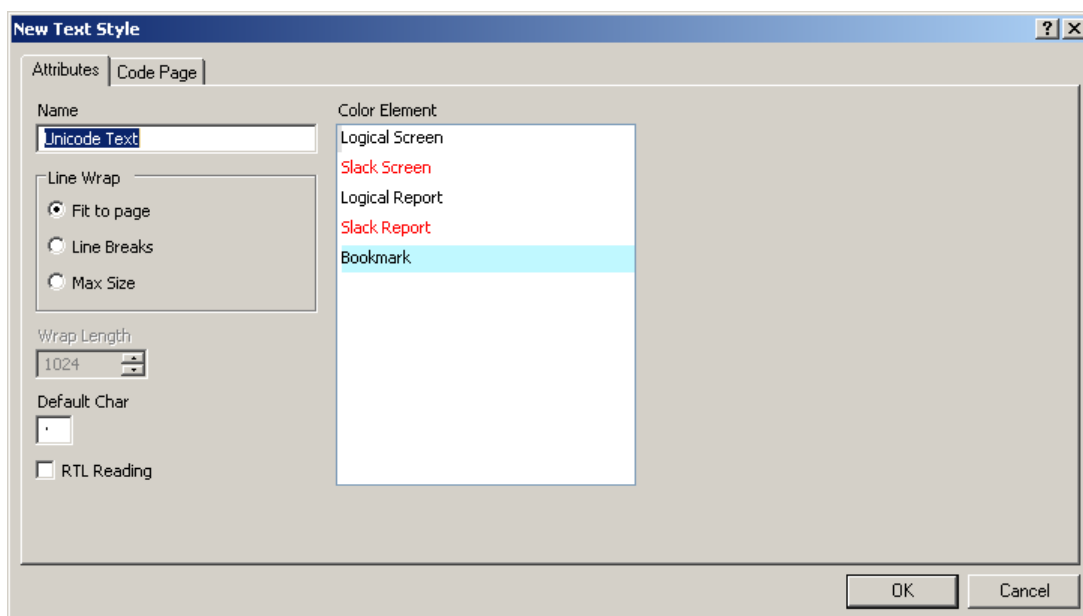
## New Text Styles Dialog

This dialog is used to define text styles that can be applied to text displayed in the Text, Transcript or Hex tabs of the View pane. This dialog consists of these tabs:

- The Attributes tab
- The Code Page tab

### New Text Styles Dialog Attributes Tab

The Attributes tab captures the text style definition.



**Name** is the name of the text style.

**Line Wrap** contains controls that determine how content appears in the Text and Hex tabs of the View pane.

**Fit to page** eliminates line breaks in displayed content, and displays all text in the window.

**Line Breaks** displays line breaks in the content.

**Max Size** ignores line breaks in the content, and wraps lines at the value set in Wrap Length.

**Wrap Length** specifies the length where a line break occurs. When you select Max Size, line breaks occur only at the value of this setting.

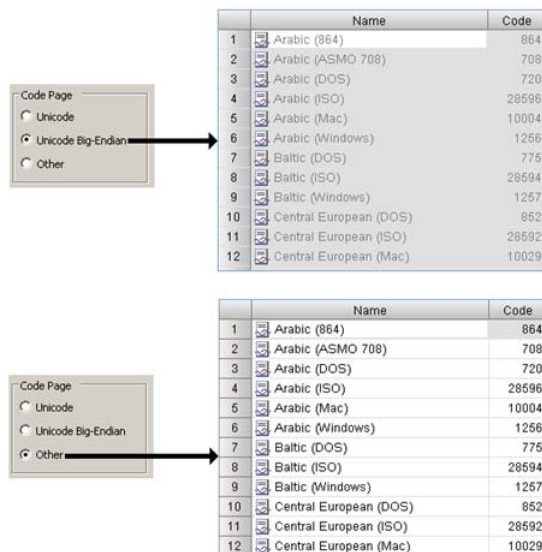
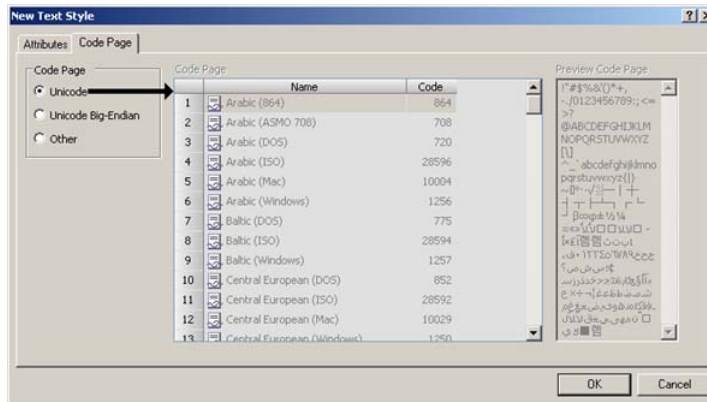
**Default Char** contains the character to use to indicate the encoding or code page could not interpret the underlying value.

**RTL Reading** sets the text display to read right-to-left (RTL).

**Color Element** contains a list of text elements that can have a color assigned to them. Double-click a list element to edit color attributes.

## New Text Styles Dialog Code Page Tab

The Code Page tab lets you select the code page for the text style you define.



**Code Page** contains settings that determines the code page type used in the text style.

**Unicode** specifies Little-Endian Unicode. If UTF-7 or UTF-8 is used, select **Other**, not Unicode.

**Unicode Big-Endian** specifies Big-Endian Unicode.

**Other** lets you select from the Code Page list.

**Code Page List** contains a list of supported code pages.

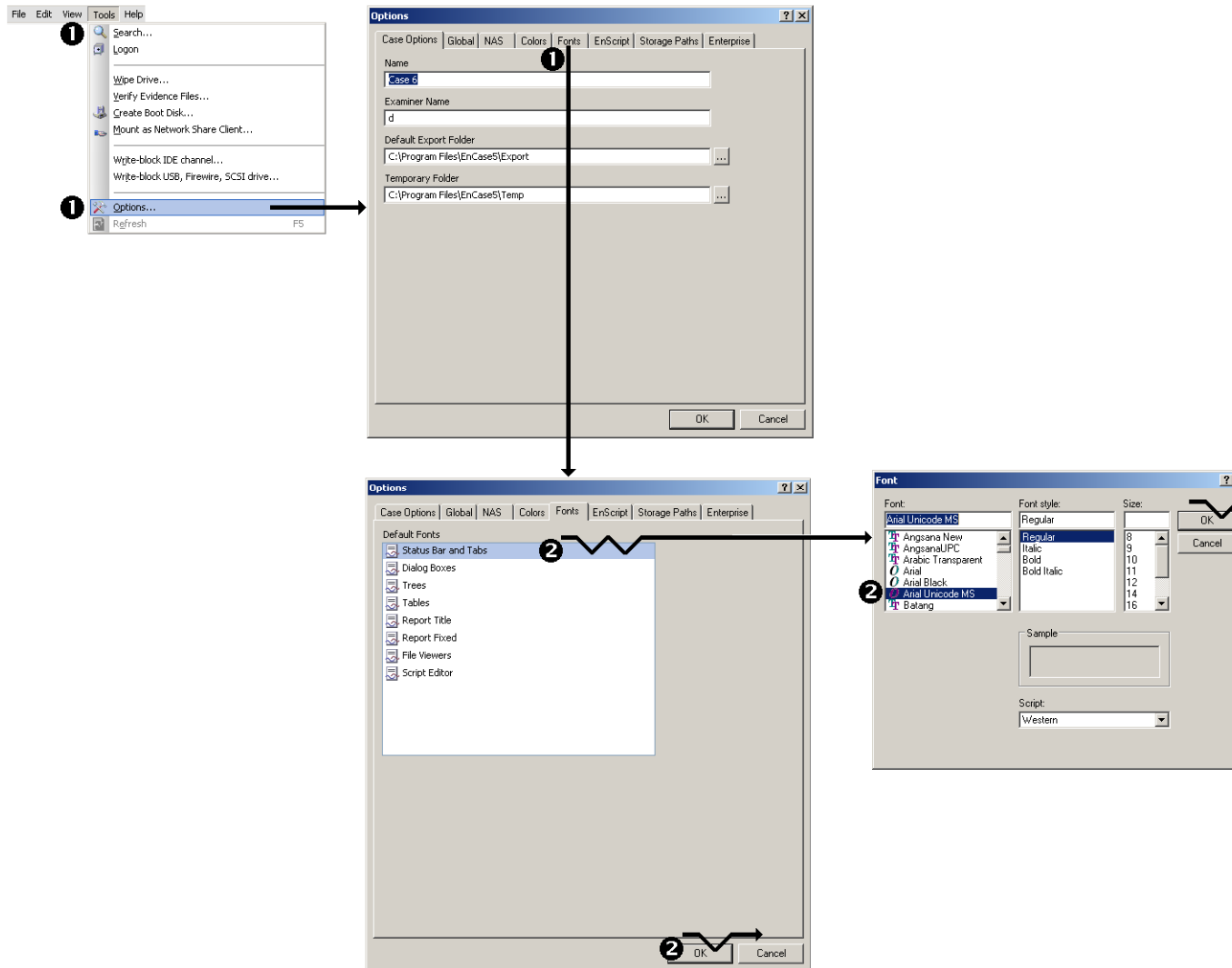
## Configuring Non-English Language Support

Non-English language support involves:

- Configuring individual interface elements
- Creating and applying text styles used on the Text and Hextabs
- Creating non-English keywords
- Creating non-English search terms
- Bookmarking non-English text
- Viewing Unicode files
- Using code pages

## Configuring Interface Elements to Display Non-English Characters

The EnCase application supports non-English language use in the interface as well as for non-English language content.



1. Click **Tools > Options > Fonts**.

The Fonts tab of the Options dialog appears.

2. For each interface element listed in **Default Fonts** where you want to display non-English:
  - a. Double-click the interface element.  
The Font dialog opens.
  - b. Change the font to *Arial Unicode MS*, and click **OK**.
  - c. Repeat step 2b until all the interface elements are configured.



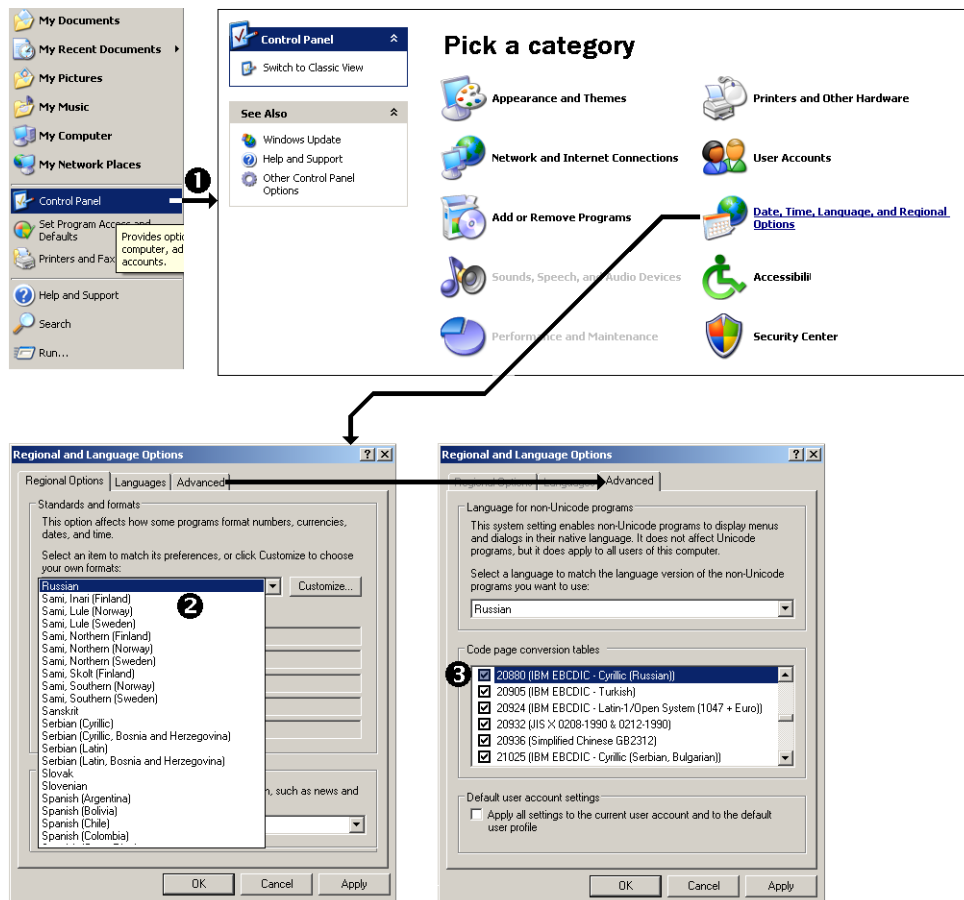
3. Click OK.

The interface is now configured to display non-English content.

## Configuring the Keyboard for a Specific Non-English Language

Windows lets you configure a keyboard for a specific non-English language. Once the keyboard is configured, you need a keyboard map or familiarity with the keyboard layout of the language.

These instructions are for Windows XP. Configuring Windows 2000, NT, and 2003 is similar.



To configure the keyboard for a specific language:

1. Click **Start > Control Panel > Region and Language Options**.

The Regional Options tab of the Regional and Language Options dialog appears.

2. In **Standards and formats**, select the desired language.
3. Select the **Advanced** tab.

The Advanced dialog appears.

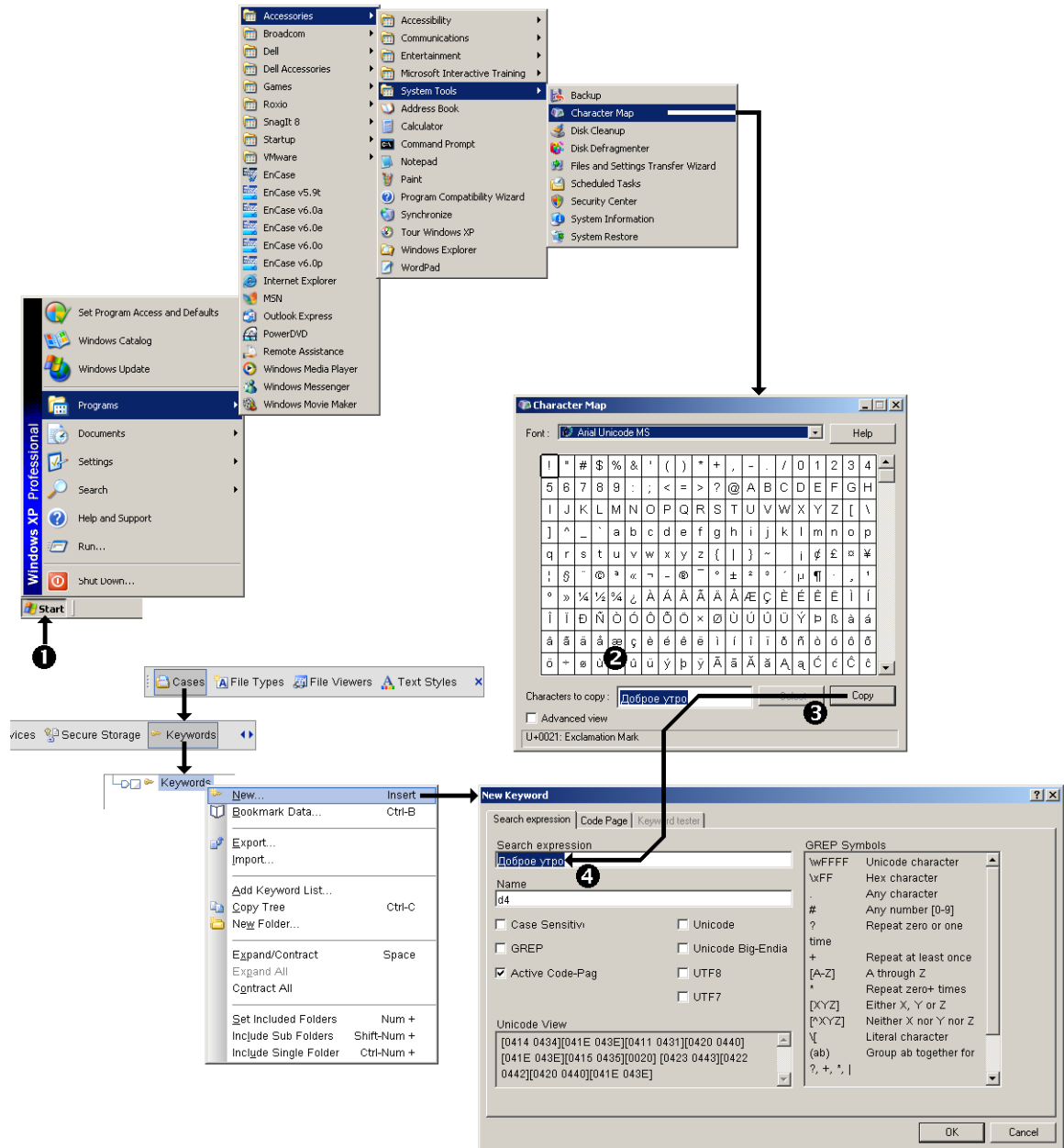
4. In **Code page conversion tables**, check the desired code page.

5. Click **OK**.

The keyboard is mapped to the selected non-English language.

## Entering Non-English Content without Using Non-English Keyboard Mapping

Windows provides a character map so you can enter non-English character strings without remapping the keyboard.



To enter non-English content using the Character Map utility:

1. Click **Start > All Programs > Accessories > System Tools > Character Map**.

The Character Map utility appears.

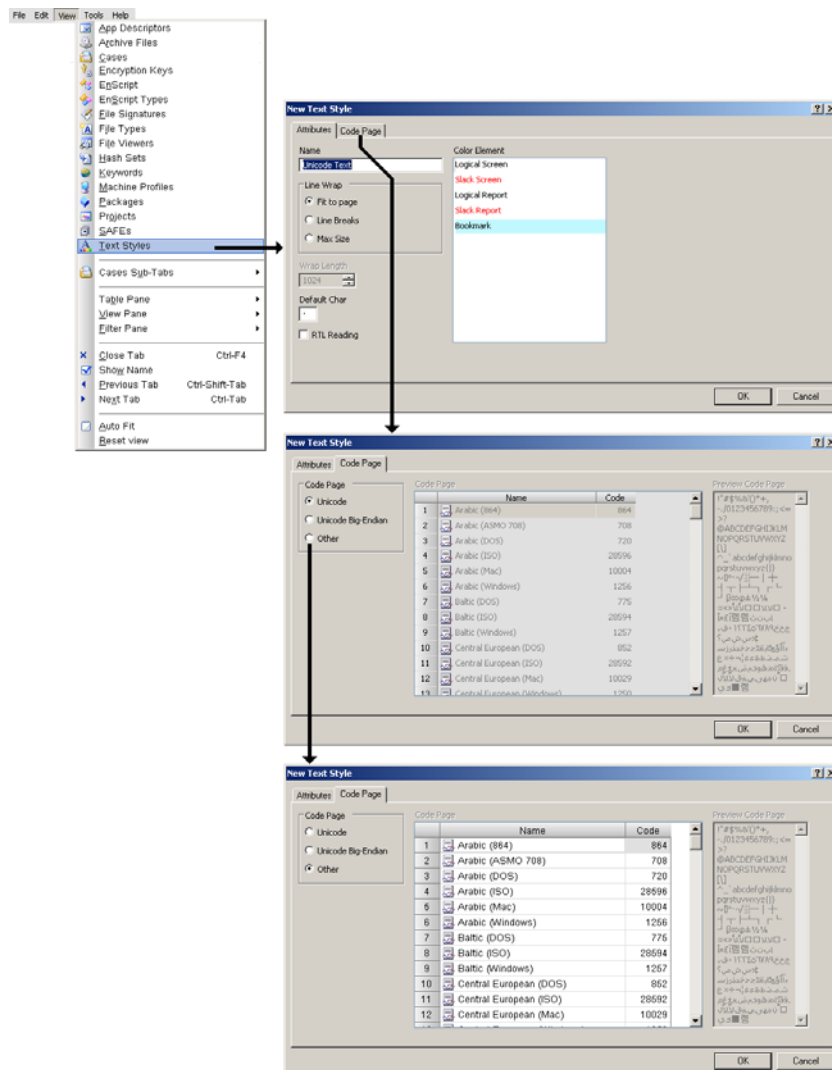
2. Click the desired character, then click **Select**.

The character is added to the **Characters to Copy** box.

3. Repeat step 2 to add more characters.
4. Click **Copy**.
5. Paste the characters where you want to use them.

## Creating and Defining a New Text Style

Text styles determine how file contents appear in the Text and Hex tabs of the View pane.



*To create and define a text style:*

1. Click **View > Text Styles**.

The New Text Style dialog appears.

2. Enter a **Name** for the new style.
3. Enter the desired character in **Default Character**.
4. Click **RTL** if the language is read right-to-left.
5. Click **OK** if you are using a code other than Unicode Big-Endian encoding. Otherwise, select the **Code Page** tab.
6. Click **Unicode Big-Endian**, then click **OK**.

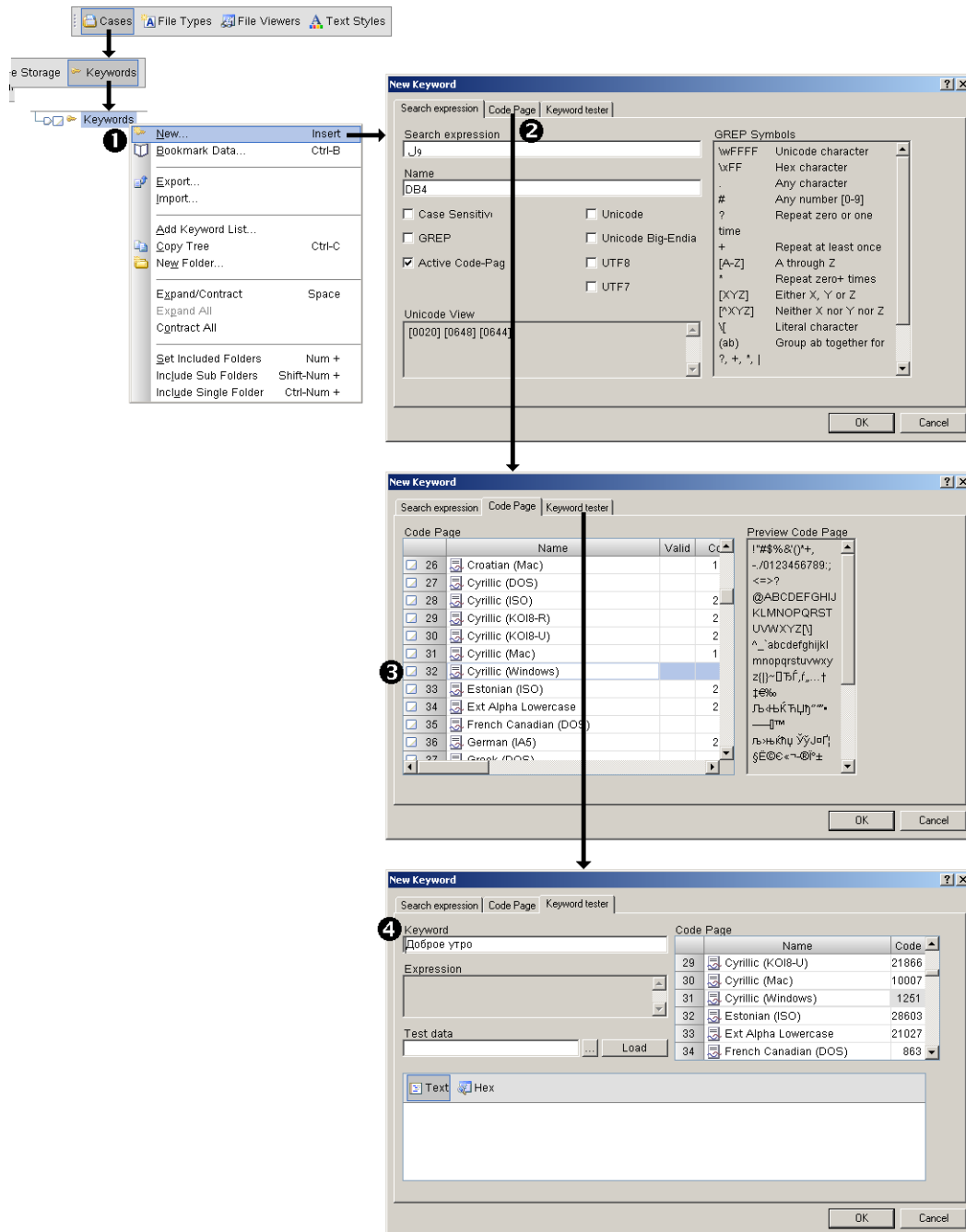
A new text style is created and defined.

If you are going to use a non-Unicode encoding:

1. Click **Other**.
2. Select an encoding from the **Code Page** list.
3. Click **OK**.

## Creating Non-English Keywords

Creating non-English keywords is the first step to take before searching non-English language content.



*To create a non-English language keyword,*

1. Right-click and select **New** from the root of the Keywords tree.

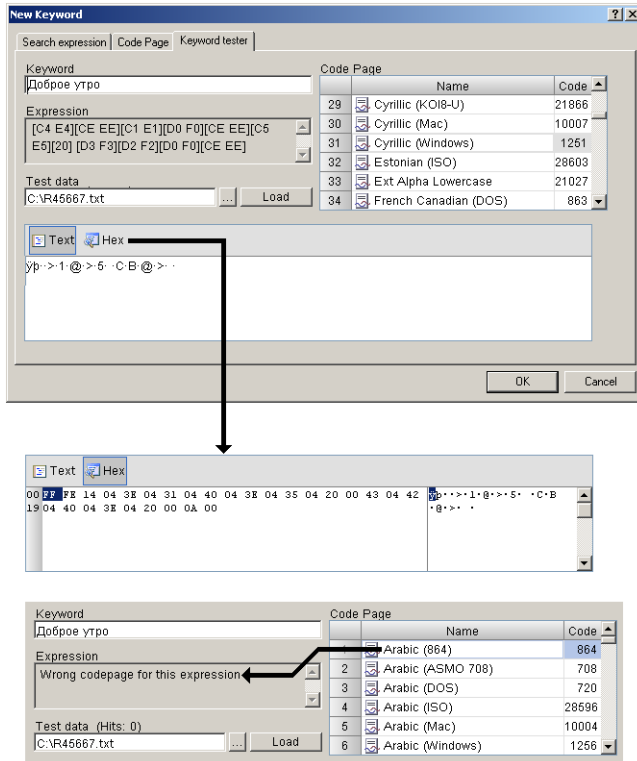
The New Keyword dialog appears.

2. Do the following on the New Keyword dialog:
    - a. Click **GREP** and enter the GREP expression into **Search Expression** to create a GREP search.
    - b. Use the Character Map to create the search string if your keyboard is not mapped to the appropriate non-English key mapping. If mapping is correct, enter the desired **Search Expression**.
    - c. Make any other selections as desired.
    - d. Do one of the following, to test the keywords:
      - If you use another code page other than the currently selected one, click **Code Page**, and proceed to Step 3.
      - Click **Keyword Tester**, then execute Step 4 to test a keyword.
  3. Click **OK**.
- The dialog closes.
4. Do the following:
    - a. Select the desired code pages from the Code Page list.
    - b. Click **Keyword Tester** to test the keyword, otherwise click **OK**.
  5. Test the keyword using the instructions in Testing a Non-English Language Keyword section, and click **OK**.

The dialog closes.

## Testing a Non-English Keyword

Open the New Keyword dialog and define the tested keyword.



*To test a non-English language keyword do the following:*

1. Enter the search expression in **Keyword**.
2. Enter or browse to the file containing the non-English language content used to test the keyword.
3. Click **Load**.  
Text appears in the Text pane.
4. If text is incorrectly rendered, select other code sheets until the text is rendered correctly. When a selected encoding is not one that was selected when the keyword was defined, the Expression field contains this message: Wrong codepage for this expression.
5. Click **Hex** to view content in hexadecimal. The values x\ FFx\ EE in the file header indicates that Unicode is the correct encoding. You may want to redefine the encoding used for this keyword.  
The hex representation of the underlying text appears.
6. Test the keyword and click **OK**.

## Querying the Index for Non-English Content

After you create an index, files that might contain non-English content can be queried using conditions.

*To query for non-English language content:*

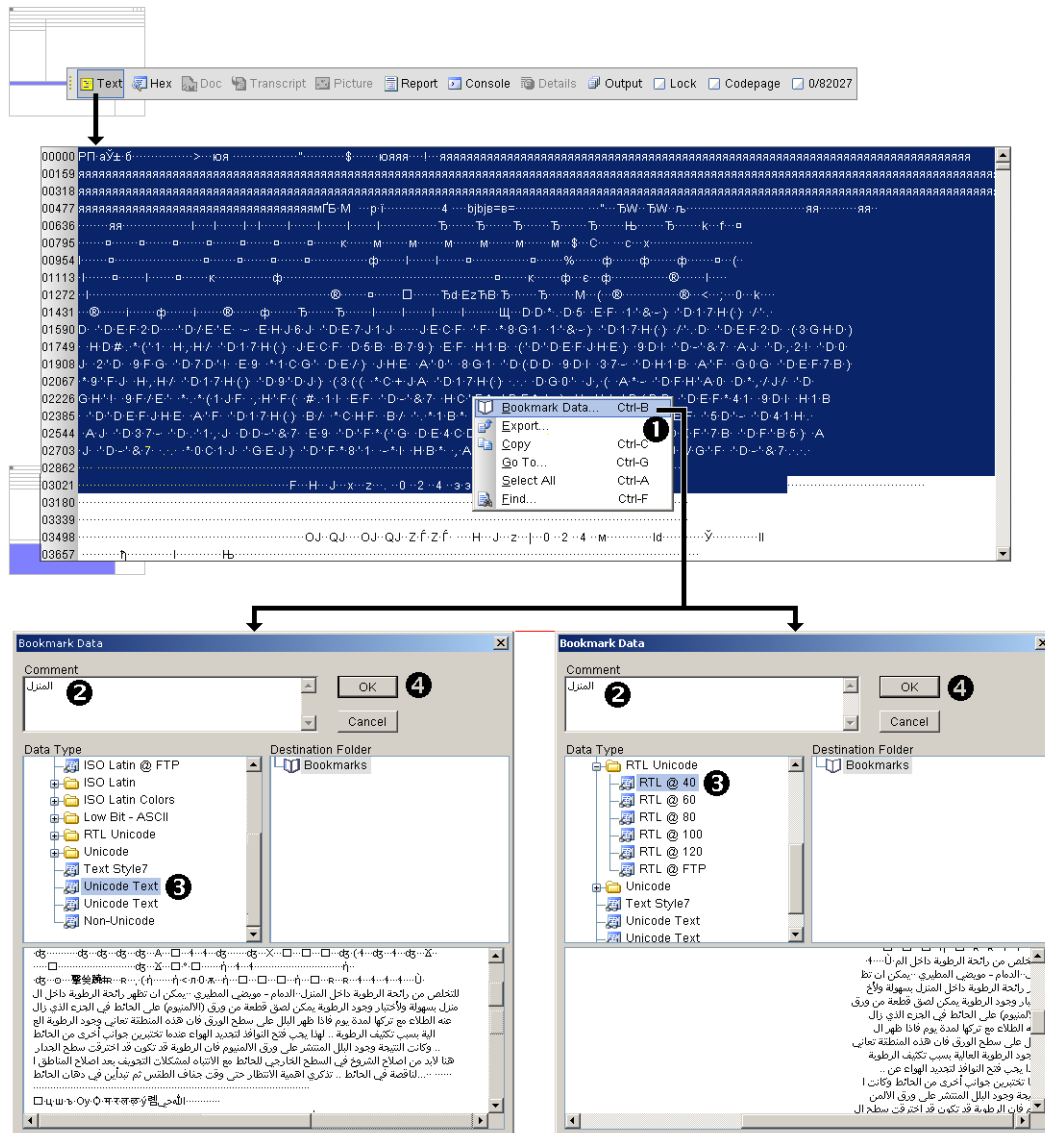


1. In the Entries tree and Entries table, select files to search.
2. Click **Tools > Index Case**.
3. In the Filters pane, click the Conditions tab.
4. Open the Index Conditions folder in the Conditions tree.
5. Select the non-English content, [for example, Index Terms (Umlaut)].



## Bookmarking Non-English Language Text

Once you find search results, bookmark them. Bookmarks associate text styles with bookmarked content.



*To bookmark non-English language text:*

1. Display the text in the View pane.
2. Sweep or select the desired text, then right-click and click **Bookmark Data**.  
The Bookmark Data dialog appears.
3. Enter a **Comment**.
4. Select the desired text style in **Data Type**.

The content appears with the selected text style applied.

5. Click **OK**.

The text is bookmarked and the dialog closes.

## Viewing Unicode Files

By default, EnCase displays characters in ANSI (8-bit) format on the Text and Hex tabs in Courier New font. Viewing Unicode files properly requires modifications to both the formatting and the font. First, the file or document must be identified as Unicode. This is not always straightforward.

Text files (.txt) containing Unicode begin with a Unicode hex signature \xFF\xFE. Word processor documents written in Unicode, however, are not so easy to identify. Typically, word processor applications have signatures specific to the document, making identification of the file as Unicode more difficult.

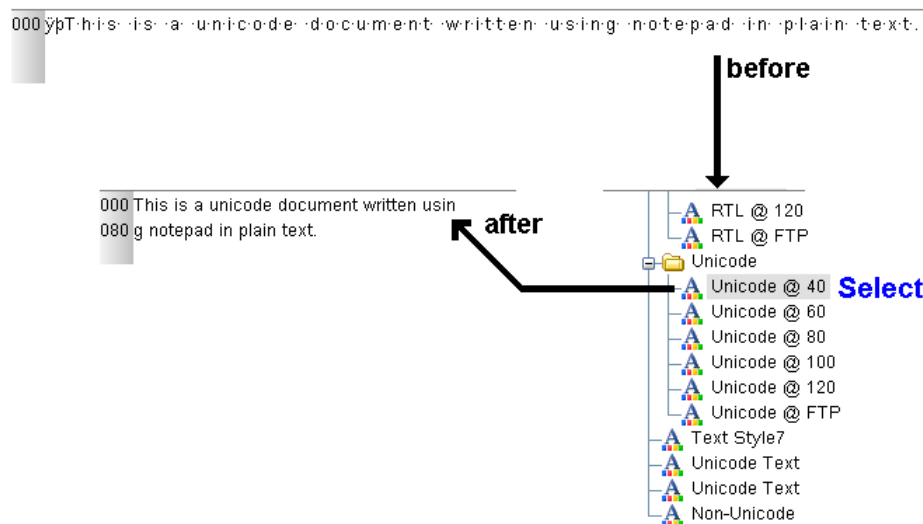


Figure 32

*To view Unicode files do the following:*

1. Click **Text Styles**.

The Text Styles tab appears in the Filter pane. Notice the default characters between the ASCII characters. The second eight bits of the 16-bit Unicode encoding cannot be translated.

2. Click the desired Unicode-based text style.

The text displayed in the Text or Hex tab is updated to reflect the new encoding.

## Viewing Non-Unicode Files

Display a file in any encoding or code page after you define it.

To view non-Unicode files:

1. Click **Text Styles** with the text displayed in the Text or Hex tab of the View pane.

The Text Styles pane appears in the Filter pane.

2. Click the desired non-Unicode based text style.

The displayed text in the Text or Hex tab updates to reflect the new encoding.

## Associating Code Pages

Non-English language files can be associated with a particular code page. A code page list is checked to prevent usage of an unavailable code page (if, for instance, a file is open on one system, then reopened on another that does not have the complete set).

If an original code page is unavailable when a file is opened, the code page association is removed. While this process is transparent, if you do open a case or mount a volume with a missing code page, a message listing the missing code pages appears.

You can associate code pages manually or automatically through Windows identification.

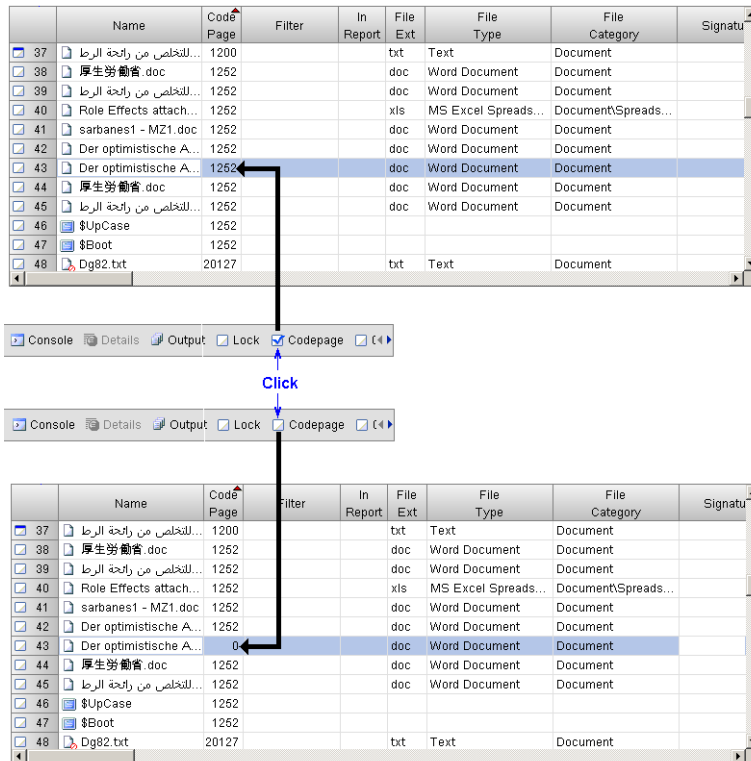
To manually set the code page:

1. Apply a Text Style with the desired code page to the entry.
2. Check the code page check box on the EnCase main window.

To have Windows automatically associate code pages to entries:

1. Select the Search button and check the Identify code page option.
2. After the search completes, the code page column populates.

To remove the association, clear the check box.



# EnScript Analysis

- EnScript Analysis 479
- Enterprise EnScript Programs 481
- EnScript Example Code 499
- Packages 505
- Send To HBGary Responder EnScript 511

## EnScript Analysis

The EnScript® language is a scripting language and Application Program Interface (API). It is designed to operate within the EnCase® software environment. Although similar to ANSI C++ and Java, not all the functions available in these languages are available. The EnScript language uses the same operators and general syntax as C++, though classes and functions are different. Classes, and their included functions and variables, are found in the EnScript Types panel in the Tree pane.

---

Note: For general information on a particular element, highlight it in the Code panel and press F1 to find the element in the EnScript Types panel.

---

EnScript programs allow investigators and programmers to develop utilities to automate and facilitate forensic investigations. The programs can be compiled and shared with other investigators. A programming background and an understanding of object-oriented programming are helpful for coding in EnScript.

---

Note: For more detailed information on the EnScript programs included with the EnCase application, refer to the EnCase Programs User Manual.

Note: For additional help in programming with the EnScript language, you can attend a training class or visit the EnScript message board.

---

## Enterprise EnScript Programs

Enterprise EnScript programs contain programs typically used with enterprise cases. Many of these programs require a SAFE to be set up to properly use them.

The available Enterprise Enscript Programs are:

**Document Incident:** used to generate a report containing the details of an incident that required investigation.

**Machine Survey Servlet Deploy:** used to manage, deploy, remove and install SAFEs and servlets to machines on the network.

**Quick Snapshot:** used to quickly take a snapshot of a machine that is currently being investigated.

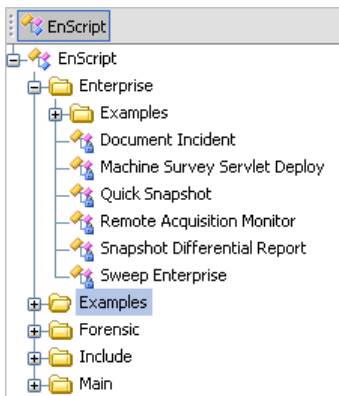
**Remote Acquisition Monitor:** used to monitor remote acquisitions between the servlets and a network storage device.

**Snapshot Differential Report:** used to report on differences of snapshots take over a period of time.

**Sweep Enterprise:** used to conduct thorough examinations on computers specified from the network tree.

To view Enterprise EnScript programs:

1. In the Filter pane, click EnScript to display the EnScript panel.
2. Open the Enterprise folder from the EnScript tree to see available scripts listed in the Table pane.



3. To run a script, double-click it in the table.

## Document Incident

Use Document Incident to generate a report containing details of an incident that required investigation.

Open a case.

1. Double-click on the Document Incident EnScript Program.
2. Enter the following details in the General Info tab:
  - ☐ Incident Reference Number
  - ☐ Primary Contact
  - ☐ Alternate Contact
  - ☐ Incident Timing

The screenshot shows the 'Document Incident' dialog box with the 'General Info' tab selected. The dialog has three tabs: 'General Info', 'Incident Details', and 'Conclusion'. The 'General Info' tab contains the following fields:

- Incident Reference Number: [Text Box]
- Primary Contact:**
  - Name: [Text Box]
  - Email: [Text Box]
  - Organization: [Text Box]
  - Department: [Text Box]
  - Address: [Text Box]
  - City: [Text Box]
  - State/Province: [Text Box]
  - Zip/Mail Code: [Text Box]
  - Phone: [Text Box]
  - Fax: [Text Box]
- Alternate Contact:**
  - Name: [Text Box]
  - Email: [Text Box]
  - Organization: [Text Box]
  - Department: [Text Box]
  - Address: [Text Box]
  - City: [Text Box]
  - State/Province: [Text Box]
  - Zip/Mail Code: [Text Box]
  - Phone: [Text Box]
  - Fax: [Text Box]
- Incident Timing:**
  - Incident Start Date: [Text Box]
  - Incident Start Time: [Text Box]
  - ☐ Incident Ongoing
  - Incident End Date: [Text Box]
  - Incident End Time: [Text Box]

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.



3. Click the **Incident Details** tab and enter information in the following fields:

- ☐ Incident Type
- ☐ Other Type
- ☐ Status
- ☐ Intent
- ☐ Incident Cause
- ☐ Incident Impact
- ☐ Affected Systems

The screenshot shows the 'Incident Details' tab of a software interface. The form is divided into several sections:

- Incident Type:** A section titled 'Check all that apply:' containing a list of checkboxes: 'Other' (checked), 'Hacking via public network', 'Hacking from internal/private network', 'Theft', 'Server compromise', 'Website defacement', and 'Equipment loss'. Below this list is an 'Other:' text input field.
- Status:** A section with three radio buttons: 'Suspected' (selected), 'Unsuccessful', and 'Successful'.
- Intent:** A section with three radio buttons: 'Accidental' (selected), 'Deliberate', and 'Unknown'.
- Incident Cause:** A large text area for describing the cause of the incident.
- Incident Impact:** A large text area for describing the impact of the incident.
- Affected Systems (note OS, IP address, and physical location):** A large text area for listing affected systems.

4. Click the **Conclusion** tab and enter the recommended course of action and comments:

The screenshot shows a dialog box titled "Document Incident" with a standard Windows-style title bar (minimize, maximize, close buttons). Inside the dialog, there are three tabs: "General Info", "Incident Details", and "Conclusion". The "Conclusion" tab is currently selected. Below the tabs, there are two text input areas. The first is labeled "Recommended Course of Action" and the second is labeled "Comments". Both areas are empty and have vertical scrollbars on their right sides. At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

5. Click **OK**

The Program generates a report. Click the name of the incident in the bookmarks panel to view the report in the table pane.

## Machine Survey Servlet Deploy

Use Machine Survey Servlet Deploy to deploy servlets to machines on the network.

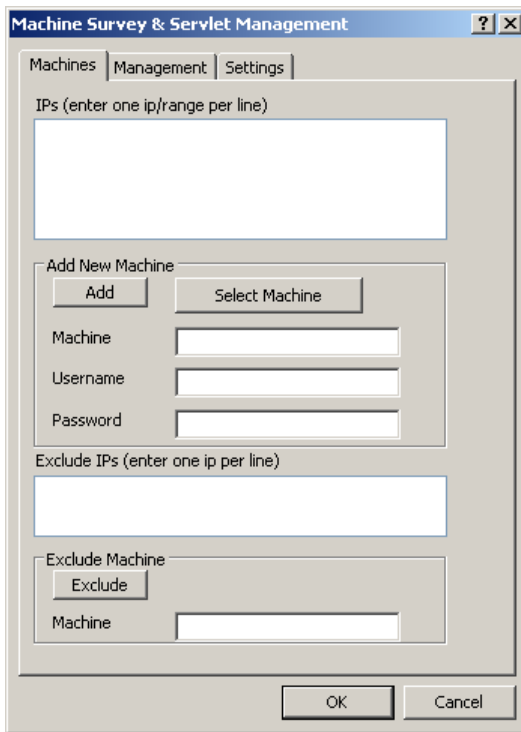
To use this method of deployment, you will need the following:

- IP addresses, or a range of all nodes where you want to deploy
- A common username and password for all nodes where you want to deploy

*To deploy servlets using Machine Survey Servlet Deploy:*

1. Open the EnCase Program.
2. Click the **EnScript** tab in the filter pane.
3. Expand the Enterprise folder by clicking the + next to it.

4. Double-click **Machine Survey Servlet Deploy**.



5. There are different ways to add to the list of machines that will receive the new servlet. Choose one or both of them below:

- ☐ Click **Select Machine**, then log on to your SAFE, select a role, and select machines using the Network Tree.
- ☐ Enter an IP address or IP Range, Username and Password and Click **Add**. If you prefer to specify an IP range using Classless Inter-Domain Routing (CIDR), you can enter it.

---

Note: If you enter an IP range, all machines must use the same username and password.

---

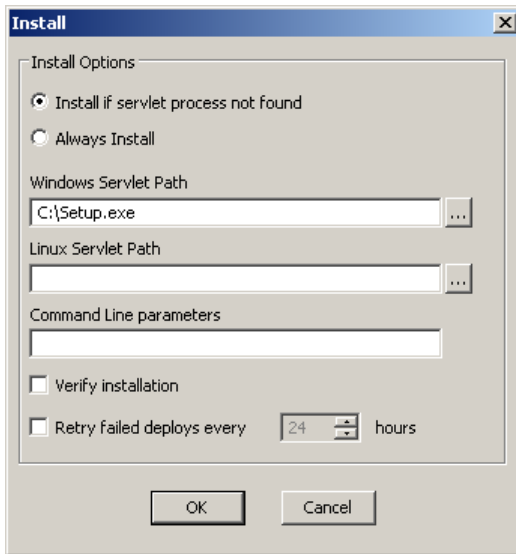
6. If you entered an IP Range and want to exclude specific addresses, enter the address in the Machine field of the Exclude Machine group and click **Exclude**.
7. Click the **Management** tab and select **Install servlet process**.

---

Note: You can also use this program to check for or stop servlet and SAFE processes. For information on how to use these features, see the *EnCase Enterprise Administrator Manual*.

---

8. Click **Install Settings**.

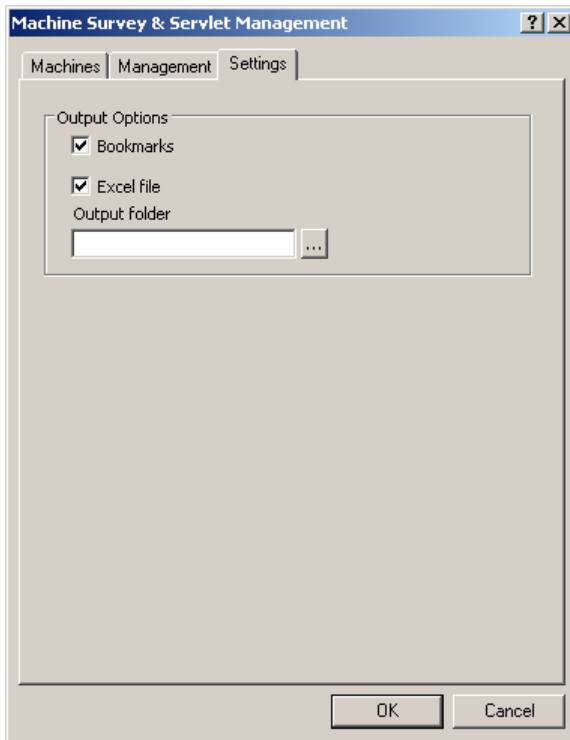


9. Complete the dialog as appropriate using the following functions:

- ☐ **Install if servlet process not found:** only installs a servlet if one is not found.
- ☐ **Always Install:** installs a servlet on all machines.
- ☐ **Windows Servlet Path:** Enter or Browse to the servlet location on your machine.
- ☐ **Linux Servlet Path:** Enter or browse the Linux servlet on your machine.
- ☐ **Command Line parameters:** Enter any command line parameters you want to use in conjunction with the servlet.
- ☐ **Verify installation:** Verifies that the install completes successfully.
- ☐ **Retry failed deploys:** Controls how often the program tries to redeploy a servlet on a machine that failed.

10. Click **OK**

11. Click on the **Settings** tab to set the output options.



12. Select an output option:

- ☐ **Bookmarks:** Outputs results to bookmarks in the current case.
- ☐ **Excel:** Outputs results in an Excel file. If you select this option, browse to or enter an output folder.

13. Click **OK**.

The program will optionally create a bookmark folder called Machine Survey Run # (With an incrementing integer). The program will also optionally create an Excel spreadsheet called MachineSurvey.xls in the folder specified above.

## Quick Snapshot

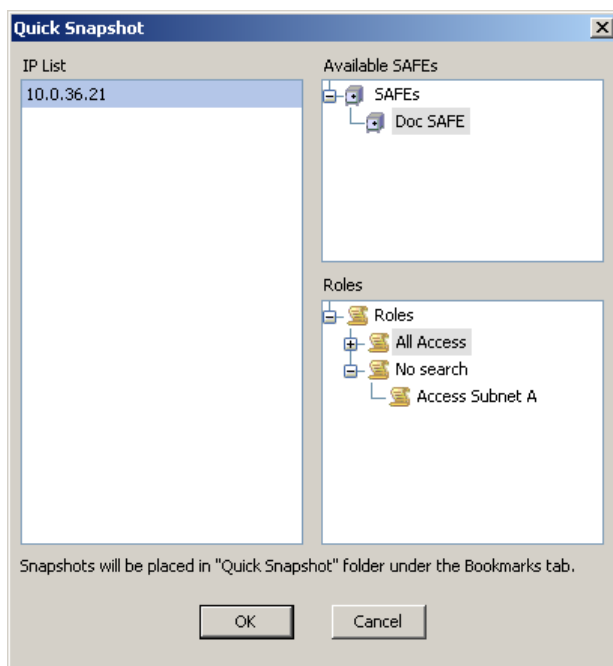
Use Quick Snapshot to quickly take a snapshot of a machine currently being investigated. Quick Snapshot does not offer a deep options set, so if you want scheduling options or the ability to run EnScript program modules while taking a snapshot, use the Sweep Enterprise program.

Before you run Quick Snapshot:

- Open EnCase and log on
- Create a case.
- Add a device to the case.

*To create a quick snapshot:*

1. Double click the Quick Snapshot EnScript Program.
2. Note the machine in the IP List, and select an Available SAFE and Role.
3. Click **OK**. Note the IP list displays the machine to be investigated using Quick Snapshot. This list is for information purposes only, and you cannot add additional nodes.



The Snapshot is created and placed in the Quick Snapshot folder in your bookmarks.

## Remote Acquisition Monitor

Use the Remote Acquisition Monitor EnScript Program to monitor remote acquisitions.

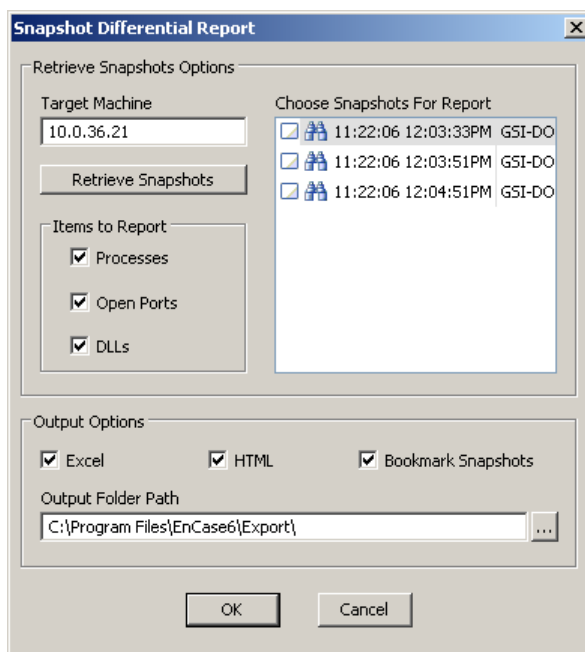
## Snapshot Differential Report

Use the Snapshot Differential Report to compare differences in several snapshots of a particular machine. It quickly detects trends of live data.

Before you begin:

- Snapshots were created and stored in a Logical Evidence File (LEF).
- Microsoft Excel must be installed.
- Add the LEF containing the snapshots into a new case.

1. Double-click the Document Incident EnScript Program.



2. Enter the name of the target machine and click **Retrieve Snapshots**.
3. In the Choose Snapshots For Report list, select the snapshots you want to compare.
4. Choose the types of items to report.
5. Choose Output Options, and provide an output path.
6. Click **OK**.

You can view results in the EnCase program, Microsoft Excel, or an Internet browser, depending on the output options you chose.

## Sweep Enterprise

The Sweep Enterprise EnScript program:

Collects data from some named subset of the network tree

- Saves the bookmarked data
- Optionally create snapshots
- Runs modules to extract data as bookmarks or exported files

If you plan to run modules, you must log on and open a case.

if you choose to deploy a servlet, both the Windows servlet and Linux servlets must be available on your machine. The Linux servlet must be available even if you do not have any Linux machines. See the *EnCase Enterprise Administrator Manual* for the paths to the servlets on your SAFE machine.

*To run the Sweep Enterprise EnScript program:*

1. Double-click on the Sweep Enterprise object in the EnScript tree on the Filters Pane.

The Case Options page of the Sweep Enterprise wizard appears.

2. If you need to change your user, or SAFE:

- a. Click **Change Safe**.

The User page of the Logon wizard appears.

- b. Select the user, enter a password (if required), then click **Next**.

The SAFEs page of the Logon wizard appears.

- c. Select the SAFE, then click **Finish**.

3. If you need to change your Role:

- a. Click **Change Role**.

The Role dialog appears.

- b. Select the desired role and click **OK**.

The Node to Sweep page of the Sweep Enterprise wizard appears.

4. If you need to change the machines swept (those that appear in **Machines**) click **Network Tree**, navigate to the appropriate subtree or machine and click **OK**.

The appropriate IP addresses appear in **Machines**.

5. Review the available modules listed in *Case Processor Modules in Forensic EnScript Programs*, then select the desired modules to run, if any, from the **Modules List**.



The Sweep Options page of the Sweep Enterprise wizard appears.

6. If servlets need to be deployed on the machines to be swept:

- a. Click **Servlet Options**.

The Servlet Options dialog appears.

- b. Click **Deploy Servlet**.

You can now change the settings.

- c. If the username and password must be updated, enter this information in **Update Machine's Username/Password**, and click **Update**.
  - d. If machines in the subtree to be swept already have servlets deployed, should not have servlets deployed, or should not be swept, enter the IP address of the machine in **Machine**, and click **Exclude**.
7. If the paths to the servlets on your machine must be changed, enter or browse to the appropriate paths.
8. Click **OK**.

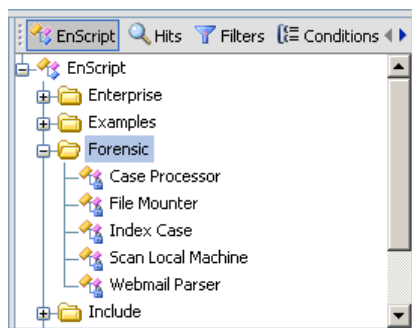
Sweep Enterprise runs and the results appear in the Bookmark table on the Bookmark Home panel.

## Forensic EnScript Code

To view EnScript programs in the EnScript panel of the Tree pane, click **View > EnScript**.

To view EnScript components in the Filter pane, click EnScripts to display the EnScript panel.

Open a folder from the EnScript object to see available scripts listed in the Table pane.

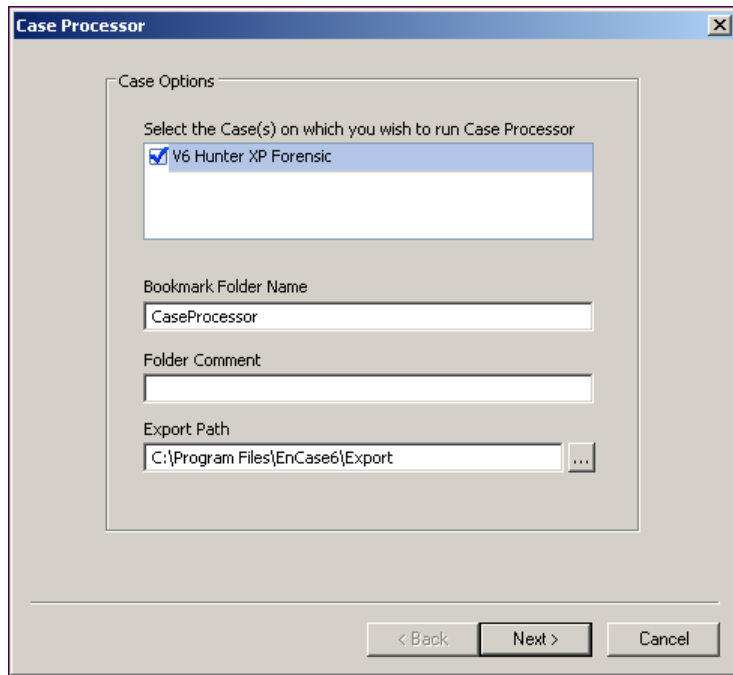


To run a script, double click it in the table.

## Case Processor

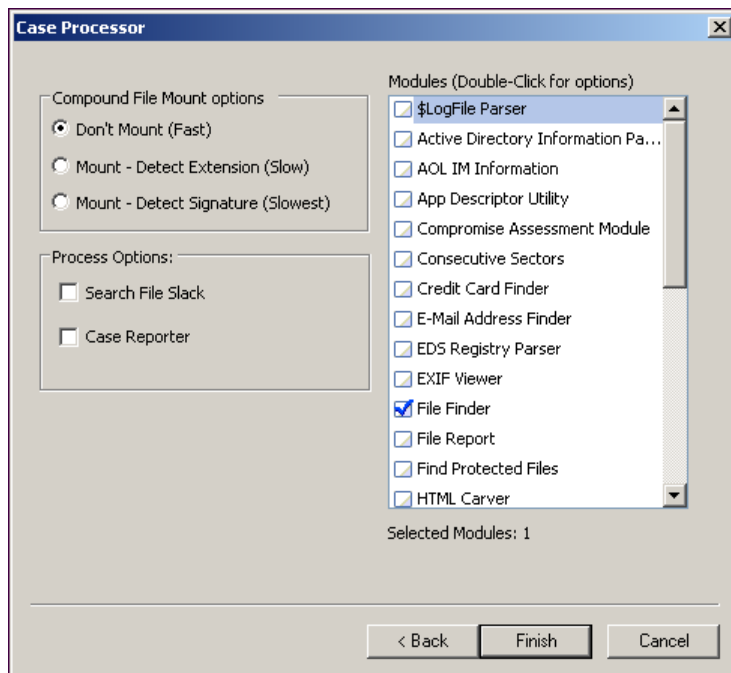
Use Case Processor to run one or more EnScript modules against an open case.

To run Case Processor, double-click the program name. A Case Processor wizard appears with the name of the open case.



1. Enter a Bookmark Folder Name.
2. Enter a Folder Comment (optional).
3. Export Path populates with the default export path.
4. Click **Next** to display the module selection wizard.

5. Make the desired selections and click **Finish**.



## Case Processor Modules

Each module available in Case Processor provides different information:

**\$Logfile Parser** parses specific information from the \$Logfile.

**Active Directory Information Parser** provides information about a directory in selected formats.

**AOL IM Information** provides data from AOL Instant Messenger data.

**App Descriptor Utility** creates app descriptor sets stored globally in the appdescriptors.ini file.

**Compromise Assessment Module** examines machines for a compromise such as a hack or virus.

**Consecutive Sectors** searches consecutive sectors filled with the same character, which characterizes attempts to wipe a drive.

**Credit Card Finder** searches an entire case for credit card numbers.

**E-Mail Address Finder** locates email addresses via a GREP search and bookmarks them.

**EDS Registry Parser** parses EDS Registry entries.

**EXIF Viewer** searches selected files for the EXIF tag and bookmarks them.

**File Finder** searches for and bookmarks selected file types.

**File Report** gathers file information on all or selected folders.

**Find Protected Files** searches a file system for files that are encrypted or require a password to open them.

**HTML Carver** searches all or selected files for keywords in HTML documents and bookmarks them.

**IM Archive Parser** searches Instant Messenger log files.

**Kazaa Log Parser** searches a case for Kazaa DBB and DAT files.

**Link File Parser** parses all or selected LCK files and retrieves selected information.

**Linux Initialize Case** locates Linux artifacts and bookmarks them.

**Linux Syslog Parser** parses Linux syslog entries and exports the data to a local drive as Excel or HTML.

**Mac Initialize Case** locates OS X artifacts and bookmarks them.

**Partition Finder** searches unused space to find deleted volume partitions.

**Recycle Bin Info Record Finder** finds and parses FAT INFO and NTFS INFO2 files.

**Scan Registry** scans the Windows registry and bookmarks artifacts.

**Time Window Analysis Module** analyses selected events between specified dates.

**Windows Event Log Parser** parses selected Windows event logs.

**Windows Initialize Case** locates Windows artifacts and bookmarks them.

**WTMP - UTMP Log File Parser** parses WTMP, UTMP, WTMPX and UTMPX files on Unix systems.

## File Mounter

File Mounter is an EnScript used to search for and mount compound files, including:

- DBX
- GZip
- PST
- TAR
- Thumbs.db
- Zip

Searches can be by extension or signature, or both.

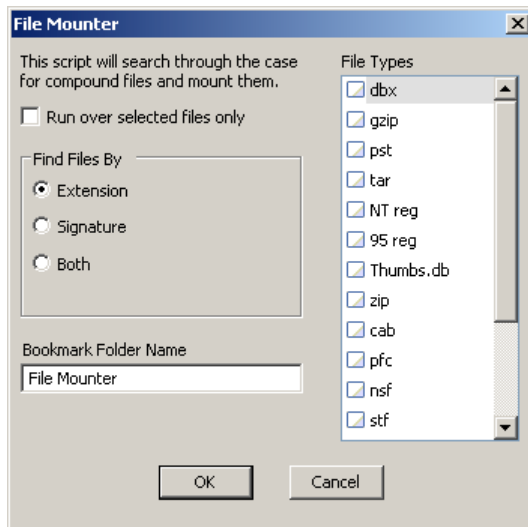
---

Note: Mounting a number of large files simultaneously can cause your system to run out of memory.

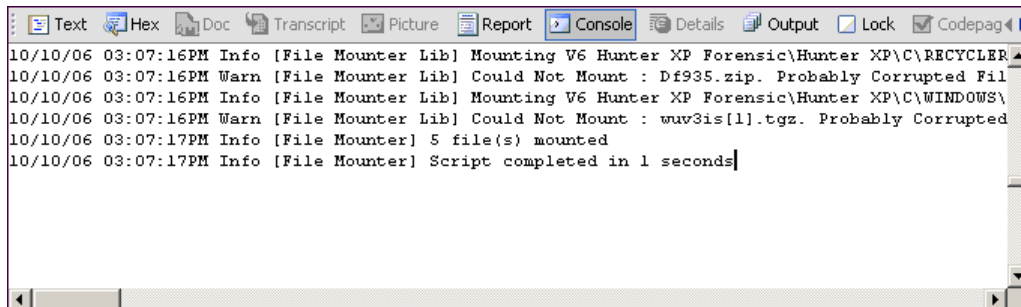
Note: Password protected files are not mounted.

---

1. Double-click **File Mounter**.
2. Select the method to find the files.



3. Select the desired file types and click **OK**.
4. To view progress, click the Console tab in the View panel.



## Compound Files

The File Mounter EnScript program lets you mount all selected compound file types, leaving them mounted at the conclusion of the EnScript program investigation.

Its main purpose is to let you catalog the contents of targeted compound files. This is a listing of items within the compound file, not the actual contents themselves.

The EnScript program finds targeted files based on the **Find Files By** and **Selected Files** options. It then catalogs the file contents into a **LogRecordClass** bookmark and adds them to the LEF if you select that option.

The program then performs a preliminary keyword search that stops after a single hit. After a hit, the file is placed into a list of files that are then mounted and completely searched.

Results appear in the Search Hits tab display.

## Mounting Compound Files

1. Select the compound files to be mounted.
2. Select any desired additional options, such as:
  - ☐ Make LEF
  - ☐ Mount Persistent
  - ☐ Search, and
  - ☐ Find Files
3. Click **OK**.

## Index Case

File indexing is part of the improved search engine. The index is a list of words in the evidence file with pointers to their occurrence in evidence. Because the index is smaller than the original evidence file it is optimized for quick searching.

To learn more about case indexing, see the *Analyzing and Searching* (see "Analyzing and Searching Files" on page 327) sections.

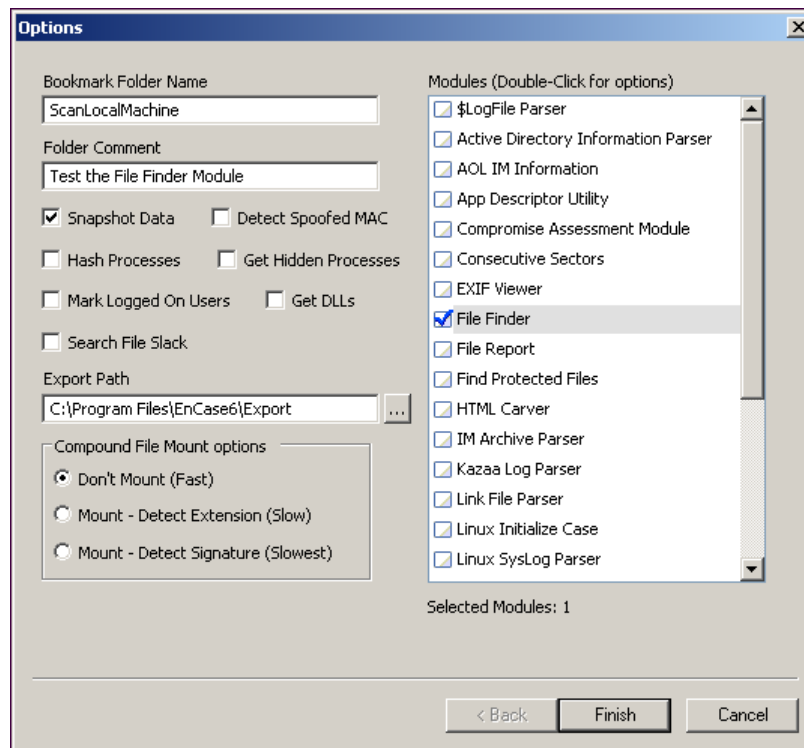
## Scan Local Machine

Scan Local Machine is an EnScript program used to run modules against a local machine.

1. Double-click **Scan Local Machine**.

It uses many of the same modules available in Case Processor.

2. Complete the options as desired and click **Finish**. Depending on the modules chosen, additional dialogs may appear open. Complete them as necessary.



---

Note: Scan local machine searches the local examiner machine and does not search the evidence within the case. If you want to search the evidence in the case, use Case Processor.

---

## Webmail Parser

Use the Webmail Parser to search the case for remnants of Web-based email.



## EnScript Example Code

In the EnScript tree in the Filter pane, the Examples folder contains example code. These programs can serve as a base for additional programming.

The COM folder contains sample EnScript programs that use COM to provide integration with MS Windows and MS Office applications. See the EnScript Program User Manual for more information.

The EnScript example programs include:

- Compound File Viewer
- Create Index Directory
- Enterprise – Using Entry Data
- Enterprise – Registry Operations
- Enterprise – Using Snapshot Data
- Find Valid IPs
- Index Buffer Reader

**Compound File Viewer** parses compound files into their constituent parts for viewing.

**Create Index Directory** generates a plain text file containing all words in an INDX file.

**FindValidIPs** finds IP addresses.

**Index Buffer Reader** parses information from an index buffer INDX file.

## COM Folder EnScript Code

The COM folder contains sample EnScript code that uses the COM API as an integration point into various other applications like MS Office or the Windows File System. Programmers use these includes to create new EnScript programs.

The COM folder contains these programs:

- Create Word Document
- File System
- Read Word Document
- Excel Create Workbook
- Outlook Read

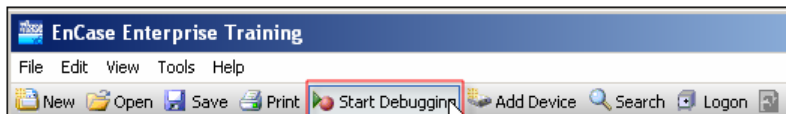
## EnScript Debugger

The EnScript debugger allows EnScript programmers to conduct runtime debugging of their programs.

After you create a project for the target EnScript program, the Start Debugging functionality is enabled:

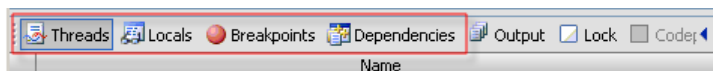


Debugging disabled (no project for the currently selected EnScript program):



Debugging enabled (there is a project for the currently selected EnScript program).

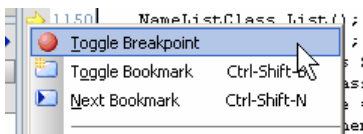
When you click **Start Debugging**, the debugger starts and opens four new tabs in the **View** Pane.



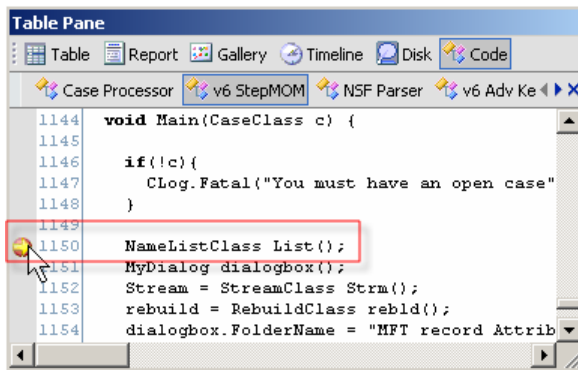
These tabs keep track of:

- currently running threads
- local variables (Locals) at the current breakpoint
- library dependencies
- breakpoint locations associated with the EnScript program

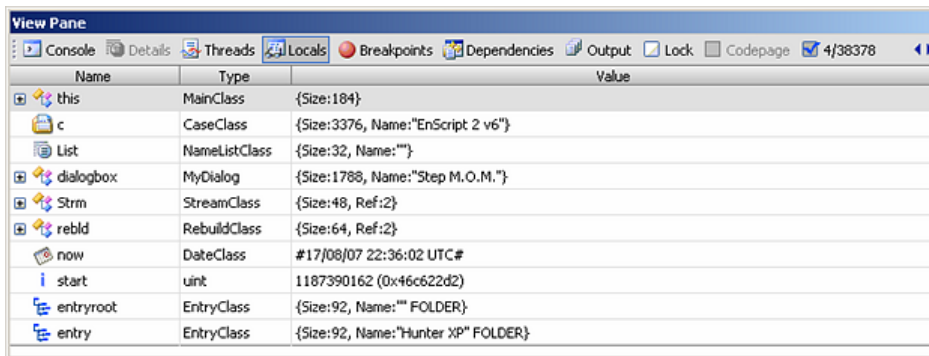
You can set breakpoints within your code. EnScript stops when it reaches a breakpoint during runtime. Use the right-click menu to set a breakpoint.



If you prefer, you can set breakpoints by left-clicking on the line number of the code.

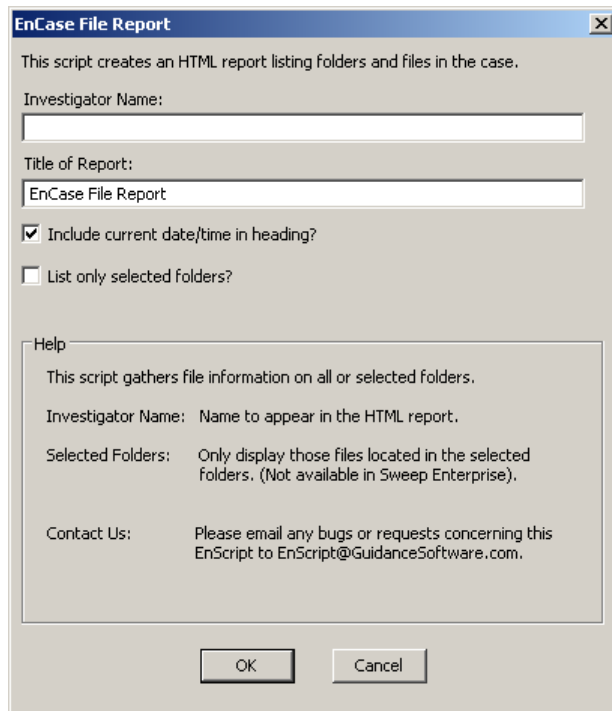


Once you set a Breakpoint, the Start Debugging button runs the EnScript program, which will stop at the Breakpoint. While stopped, you can analyze the runtime information in the new tabs in the View Pane.



## Help for EnScript Modules

The Case Processor, Sweep Enterprise, and Scan Local Machine screens contain a Help button or Help section for each available module.



## EnScript File Mounter

The File Mounter program catalogs the contents of selected compound files (for example, .zip files). This produces a listing of the items in the compound file, not the actual file contents. The program duplicates the structure of compound files into Log Record bookmarks.

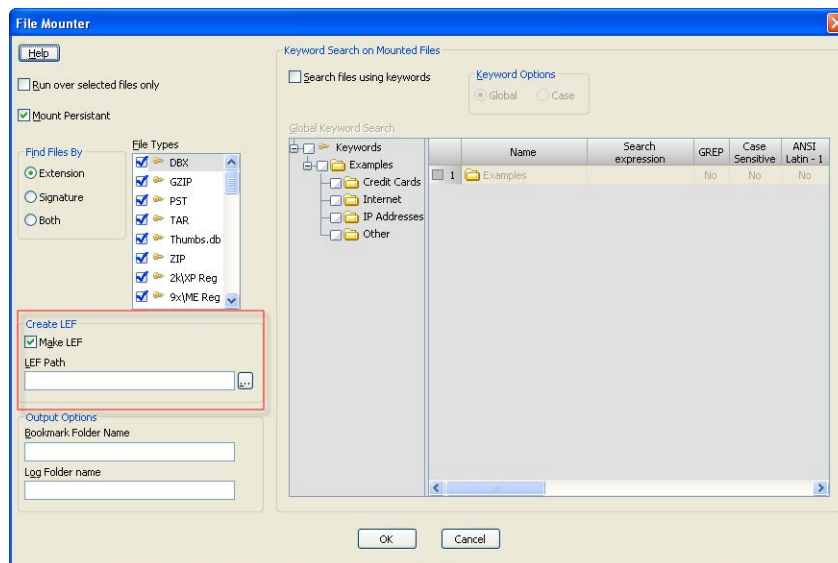
You define the types of files to process and the criteria. You can select file types by file extension or signature.

You can choose to mount them persistently (leaving them mounted after the conclusion of the EnScript program) or non-persistently. The non-persistent option returns them to their unmounted state when the EnScript File Mounter program completes. Other options include:

- The ability to create a Logical Evidence File (LEF) that includes the contents of all mounted files
- Creating a keyword search of the targeted files

All files having at least one keyword hit will be mounted persistently and their corresponding search hits display in the Search Hits tab.

Certain Microsoft Office documents are considered compound files. You can parse their metadata and search it. For example, you can locate and bookmark Microsoft Word document metadata (edit times, page numbers, word counts, etc.). File Mounter bookmarks Authors as text and Edit Times as dates.



## Include EnScript

The Include folder contains common program code shared by other higher-level EnScript components. These scripts are not executed independently. They are meant to be used or included in other scripts.

Right now, there are nearly 100 include files in this software. They are stored by default in `C:\Program Files\EnCase\EnCase\EnScript\Include`. They can, however, be stored in another folder within `... \EnScript\`. An EnScript developer creating new include files to work with new EnScript component can create a new folder and place the new include programs there.

Once the new folder is created, EnCase® applications must know of its location.

1. Click **Tools > Options > EnScript** to see the Options dialog.



2. Change the Include Path field entry to reflect the new include folder location.

---

Note: Add only the folder name, not the complete path.

---

## EnScript Help

There are currently two sources of information about EnScript programs.

- **Help > EnScript Help**
- **View > EnScript Types**

## EnScript Types

EnScript types reference resources containing the EnScript language classes. Perusing these types provides information about EnCase classes and functions.

Click **View > EnScript Types**

The Tree pane contains a list of the classes. Selecting the Report panel of the Table pane displays a read-only description of the selected class.

## Packages

Packages are a way to distribute EnScript programs without allowing others to view or modify the code. This allows for centralized source control, and avoids unwanted code sharing. Packages are built with the .enpack file extension and function to end users exactly as EnScript programs. In addition to blocking the code from end users, you can also create license files specific to license keys, protecting you from unwanted duplication. The license files extension is .EnLicense.

## Package Features

Features that support the packages include:

- New Package dialog
- Create License dialog

Use the New Package dialog to create, build and edit packages. When building or editing packages the name of this dialog changes, but the panels and setting remain the same.

Use the Create License dialog to create licenses for a package. The license is assigned the **License Name** value on:

- The Package panel of the New Package dialog
- Edit <package name> dialog
- The Build dialog.

## New Package Dialog

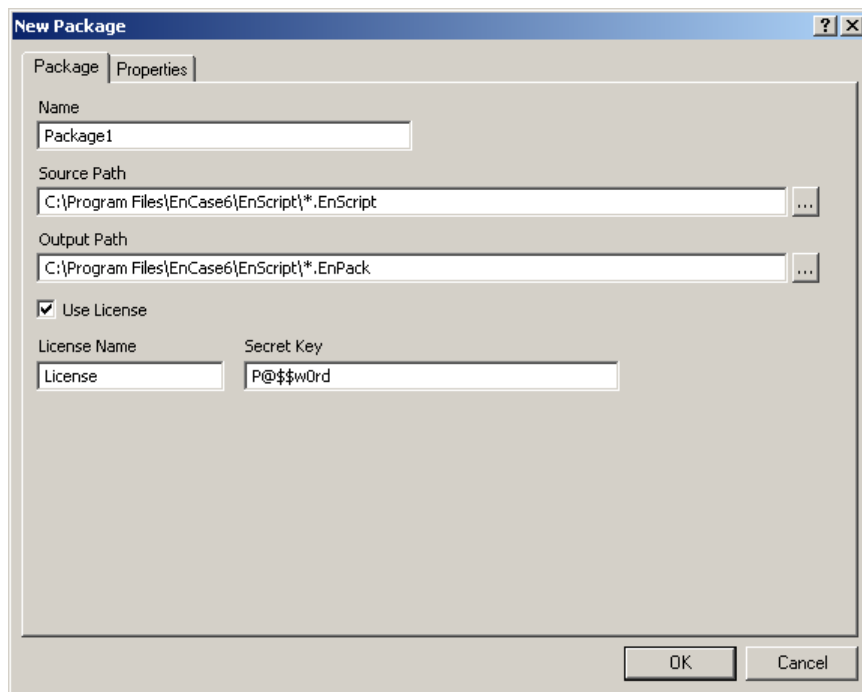
The New Package dialog contains:

- A package panel
- A properties panel

Use the New Package dialog to create, build, edit, and run packages.

## Package Panel

The Package panel of the New Package dialog captures attributes related to the package. Use this panel to create, build, and edit the package.





**Name** is the file name of the package, as seen in the interface.

**Source Path** contains the path to and filename of the EnScript source code to be packaged.

**Output Path** contains the to and filename of the package or package to be created.

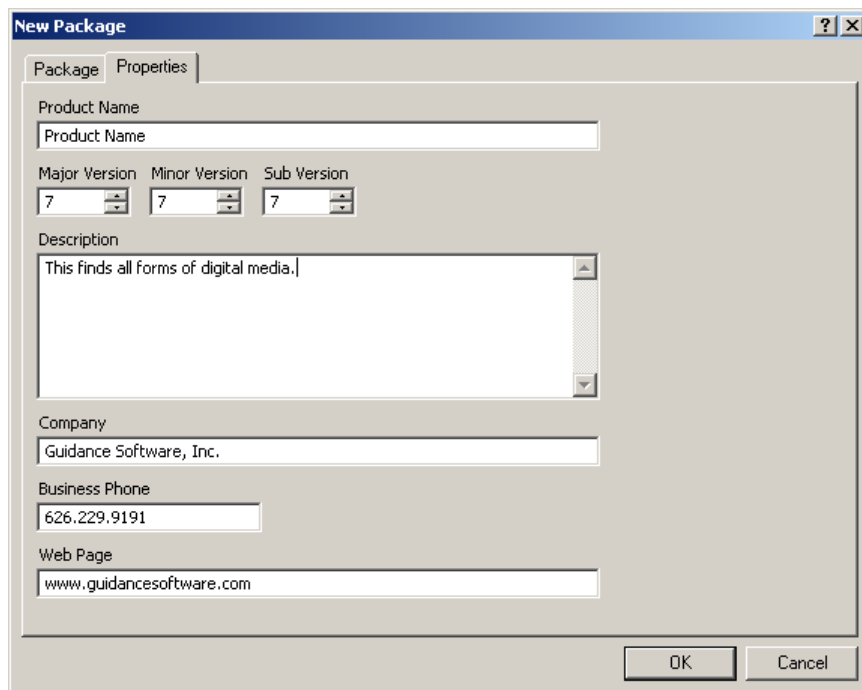
**Use License** determines whether other license related controls appear on the dialog. Use this setting if you want to license the package.

**License Name** contains the filename of the license without its file extension. This setting only displays when **Use License** is selected.

**Secret Key** is a key used in conjunction with the license file to secure the code within the package. This text is not exposed to end users and should not be given to end users.

## Properties Panel

The Properties panel of the New Package dialog captures attributes related to the product being packaged. This panel is used to create, build, and edit the package.



The screenshot shows the 'New Package' dialog box with the 'Properties' tab selected. The dialog has a title bar with a question mark and close button. The 'Package' tab is also visible. The 'Properties' tab contains the following fields:

- Product Name:** A text box containing 'Product Name'.
- Major Version:** A spin box set to 7.
- Minor Version:** A spin box set to 7.
- Sub Version:** A spin box set to 7.
- Description:** A text area containing 'This finds all forms of digital media.' with a vertical scrollbar.
- Company:** A text box containing 'Guidance Software, Inc.'.
- Business Phone:** A text box containing '626.229.9191'.
- Web Page:** A text box containing 'www.guidancesoftware.com'.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

**Product Name** is the name of the EnScript source code.

**Major Version** is the major version number of the EnScript source code.

**Minor Version** is the minor version number of the EnScript source code.

**Sub Version** contains identifiers for bug fix versions, patches, or build numbers of the EnScript source code.

**Description** is self-explanatory.

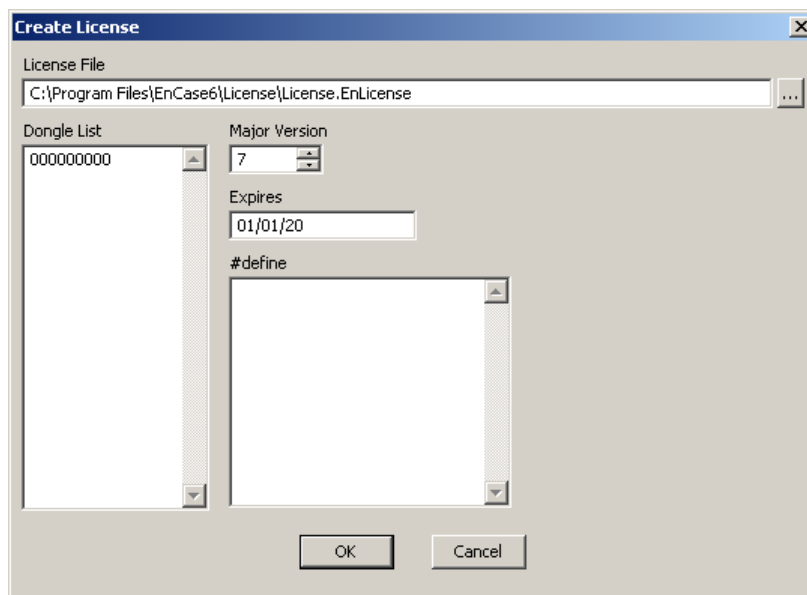
**Company** is the name of the company associated with the package.

**Business Phone** is the phone number of the company associated with the package.

**Web Page** is the URL of the company Web page associated with the package.

## Create License Dialog

Use the Create License dialog to create a license associated with a package. The association is made by entering the filename contained in **License File** without its extension.



**License File** contains the path to and the filename of the license file.

**Dongle List** contains the dongle numbers that enable the license. If the license is not restricted, leave this setting blank.

**Major Version** contains the major version number of the software release.

**Expires** contains the date when the license will expire.

**#define** contains names used in the code, defined using the #define directive, which associate the license with specific functionality. A subset of functionality is associated with a given license.

## Using a Package

A package is

- Created
- Edited
- Built
- Run

In addition, one or more licenses are created and associated with a package.

## Creating a Package

To create a package

1. Do one of the following:
  - ☐ Click the **Packages tab**, adjacent to the **Cases tab** on the root toolbar of the Tree pane.
  - ☐ Click **View > Packages**
2. Right-click on the Packages tree in the Tree pane, and then click **New**.  
The New Package dialog appears displaying the Package panel.
3. On the Package panel, complete the settings, and then click **Properties**.  
The Properties panel appears.
4. On the Properties panel, complete the settings, and then click **OK**.

Once created, the package appears in the Packages Table in the Table pane. The columns in this table contain the details entered in the New Package dialog.

Table   Report   Code										
	Name	Filter	In Report	Major Version	Minor Version	Sub Version	Source Path	Output Path	License Name	Secret Key
1	Package1			7	7	7	C:\Pr...	C:\Pr...	License	P@f...

---

Note: Creating a package does not produce the package file. To produce the package file, see [Building a Package](#)

---

## Editing a Package

1. In the Package table on the Table pane, double-click on the desired package.  
The Edit <package name> dialog appears.
2. Modify the settings as desired, and click **OK**.

---

Note: If you want to change the code, you will need to first modify the EnScript code source file, and then generate a new package file. You may want to alter the version numbers to reflect this.

---

## Building a Package

1. In the Package table on the Table pane, double-click on the desired package.  
The Edit <package name> dialog appears.
2. Modify the settings as desired, and then click **OK**.

The package is now created in the output path specified.

## Creating a License

You can create a license can be created independently of its associated package. The association with a package is made when you define the package.

*To create a license for a package:*

1. In the Package Table in the Table pane, right-click the package and click **Create License**.  
The Create License dialog appears.
2. In **License File**, enter or browse to the path and filename.
3. In the **Dongle List**, enter the license keys.
4. In **Major Version**, select the appropriate version number.
5. In **Expires**, enter the expiration date of the package.

6. If you want to control the feature set used via this license, in **#define**, enter the #defined names associated with the feature set.
7. Click **OK**, and then click **OK** again in the status message box.

## Running a Package

Create and build a package. A license may be associated with the package as well.

### *To run a package*

1. Copy the created license file to `C:\Program Files\EnCase6\Licenses`.
2. Do one of the following:
  - ☐ Change root folder of your EnScript folder to reflect the location of the package created.
  - ☐ Copy the created package to a folder in your current EnScript root folder, normally `C:\Program Files\EnCase6\EnScript`.
3. If a license is associated with the package, ensure that the installed security key matches the key(s) entered when creating the license.

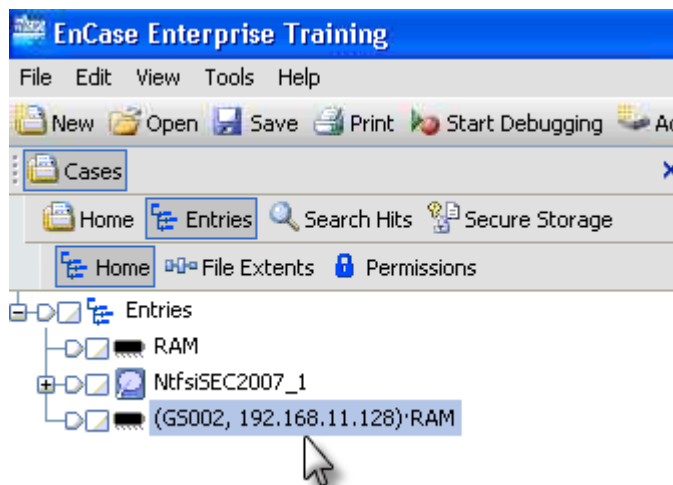
The EnScript program is now ready to run.

4. In the EnScript tree in the EnScript panel of the Filter pane, double-click the package to run it.

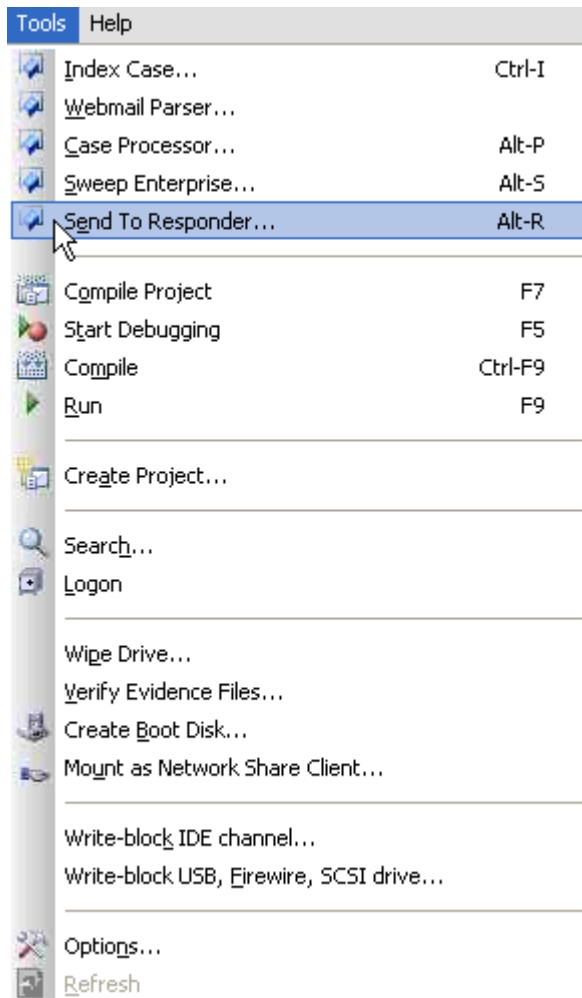
## Send To HBGary Responder EnScript

This EnScript passes a memory object gathered by EnCase to HB Gary's Responder software.

1. Select the physical memory to send:



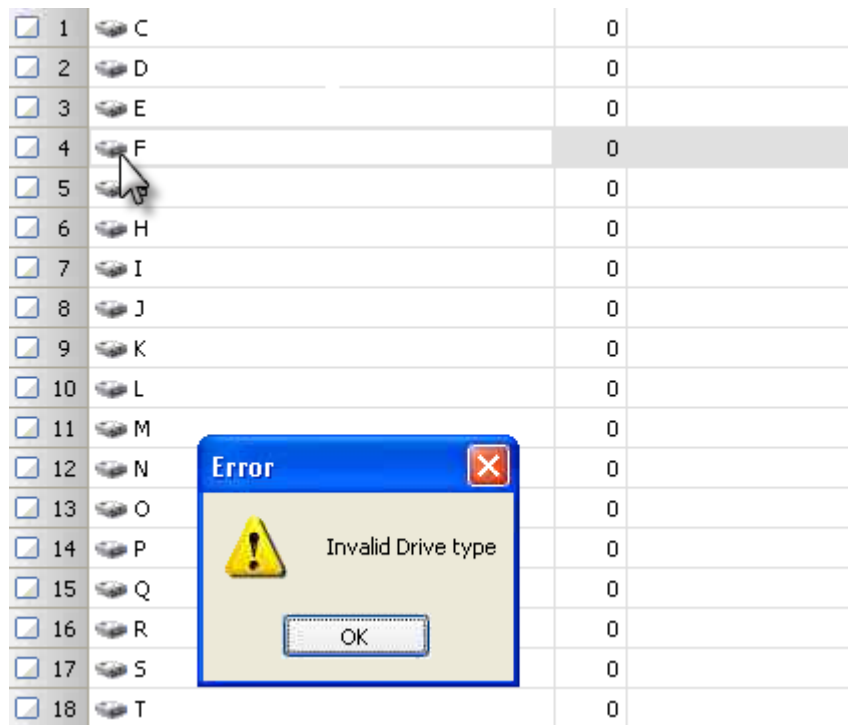
2. Click **Tools**→**Send To Responder**:



3. EnScript drops the physical evidence device information, byte for byte, into a flat file and sends it to Responder. Here is an example of the file viewed in Windows Explorer:

Name ▲	Size	Type	Date Modified
(G5002, 192.168.11.128)·RAM.memDump	523,760 KB	MEMDUMP File	4/10/2008 2:05 PM

If you specify a device or file other than a physical memory drive, an error message displays:



HBGary Responder does not support analyzing Windows Vista memory dump.





# Using EnCase Tools

- Toolbar 516
- Tools Menu 517

## Toolbar

The toolbar contains icons for the most frequently used EnCase® functions.

When you open EnCase® in acquisition mode, only the **New**, **Open**, **Print**, and **Refresh** icons display in the toolbar. When you open a case, the **Add Device** icon displays.

There is a corresponding menu command for each toolbar icon.

When the toolbar is wider than the main window, the toolbar wraps to another line.

Some of the icons are enabled only when they are useful, such as **Print** and **Refresh**.

The panes and the tabs in the toolbars also display context-dependent icons, accessed from right-click menus.

**New** opens the Case Options wizard for defining a new case.

**Open** displays a dialog for opening an existing case.

**Print** opens the Print dialog.

**Refresh** updates a list or table to reflect changes in the file system.

**Save** opens the Save dialog.

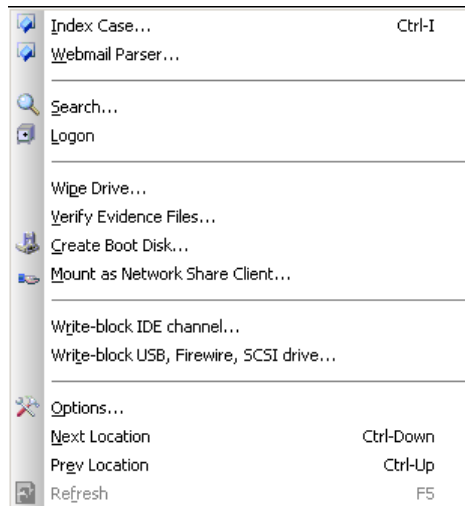
**Add Device** opens the Add Device wizard.

**Search** opens the Search dialog, so you can search evidence associated with the case.

Other icons display depending on their context. There is always a corresponding menu command.

## Tools Menu

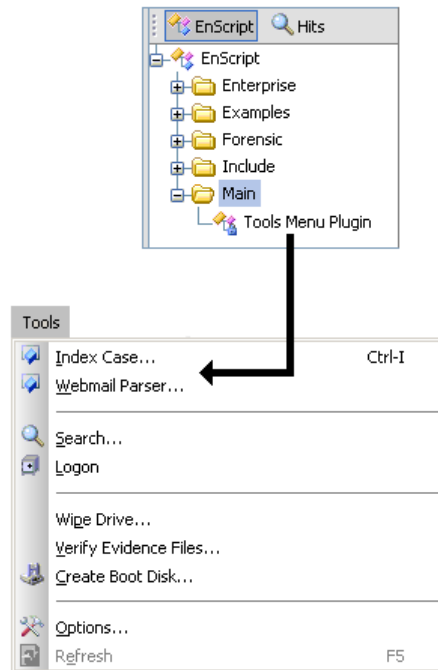
The Tools menu, at the top of the display contains commands for various utility programs.



## EnScript Programs Shortcut Submenu

The shortcut submenu contains shortcuts to EnScript programs that are designated in the Tools Menu Plugin. The Tools Menu program is in the EnScript panel of the Filter pane. You can modify it to include additional shortcuts from the tools menu.

The EnScript Program Shortcuts and the EnScript Program that Provide the Related Command Functionality



## Wipe Drive

---

**Warning!** This procedure completely erases media and overwrites its contents with a hexadecimal character. Invoke Wipe Drive with extreme care.

---

---

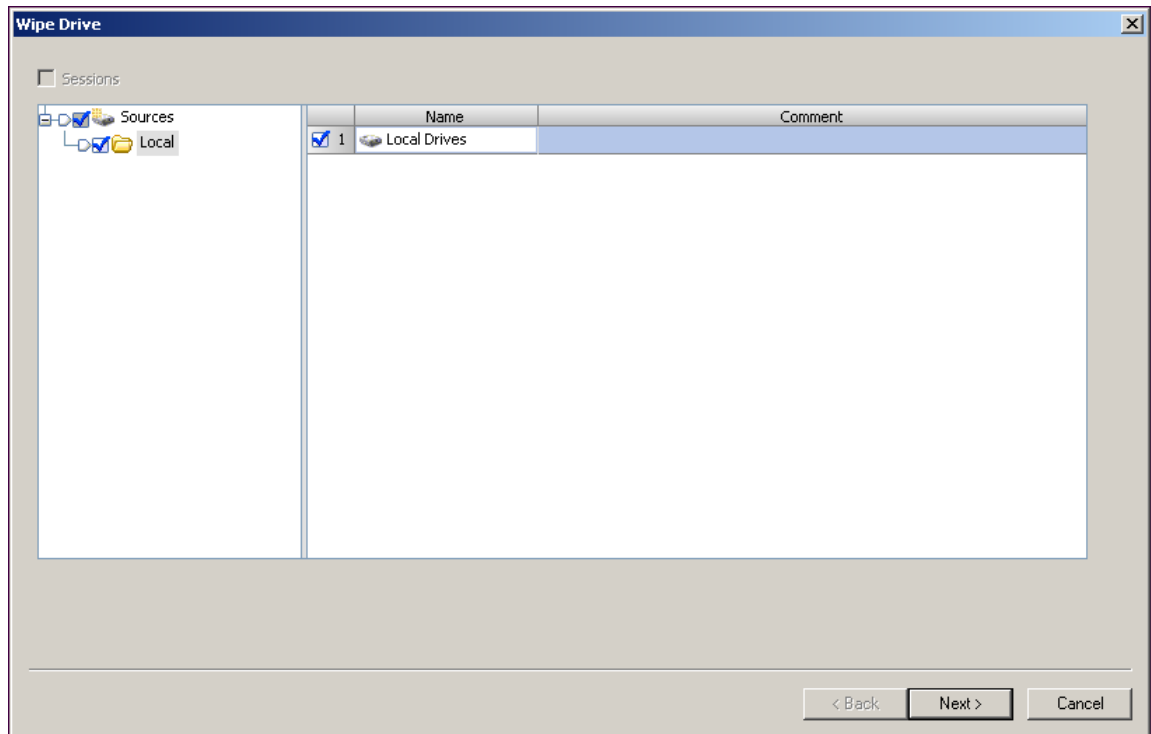
Note: Execute the Wipe Drive utility to remove all traces of any evidence files from a storage drive.

---

*To wipe a drive:*

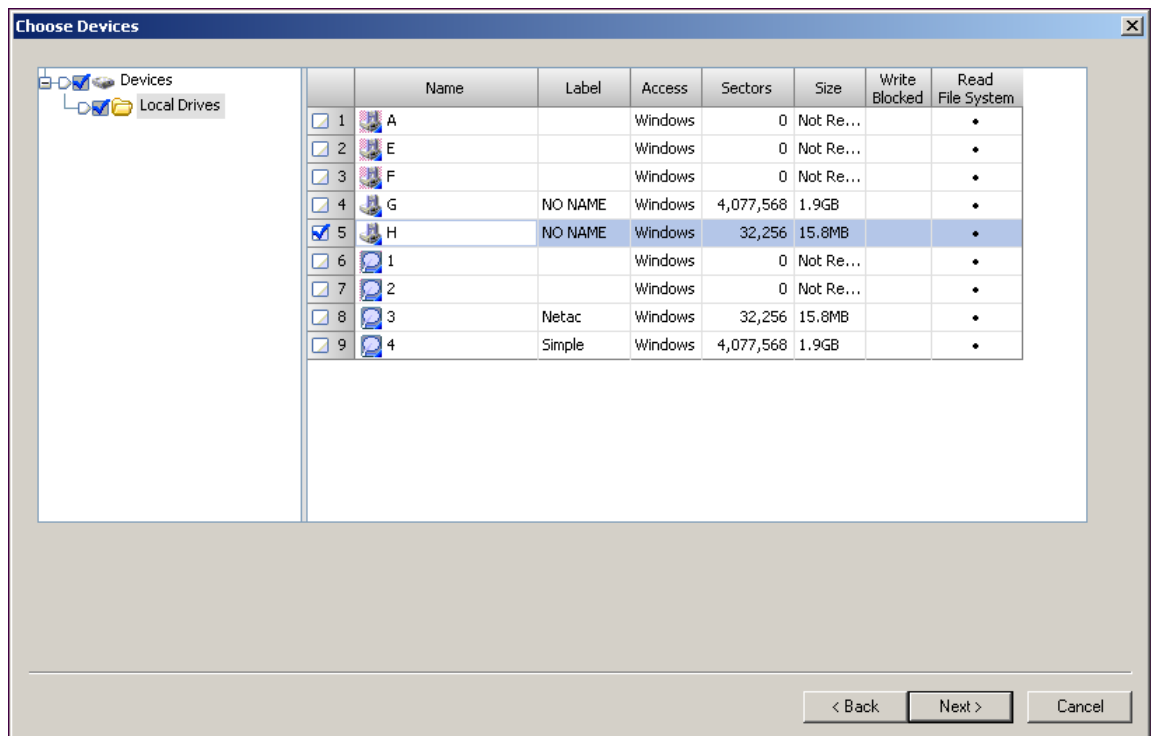
1. Click the **Wipe Drive** option on the Tools menu.

The drive selector displays.



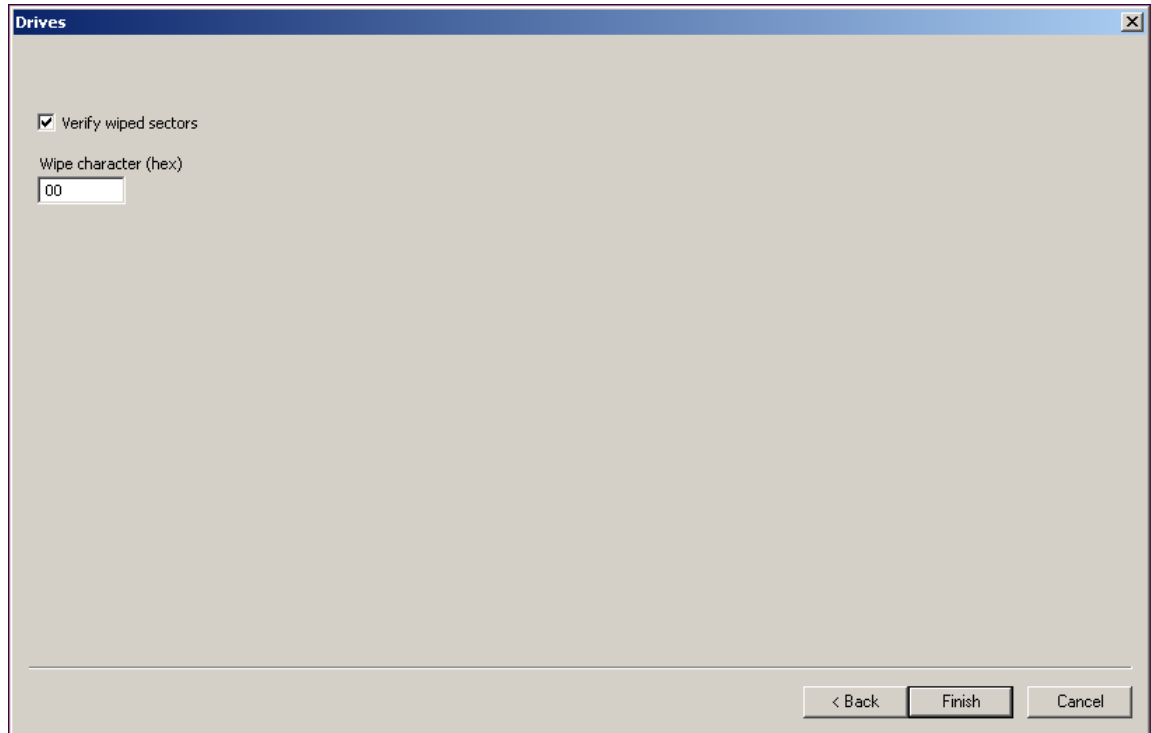
2. Make initial selections and click **Next**.

The Choose Devices screen displays.



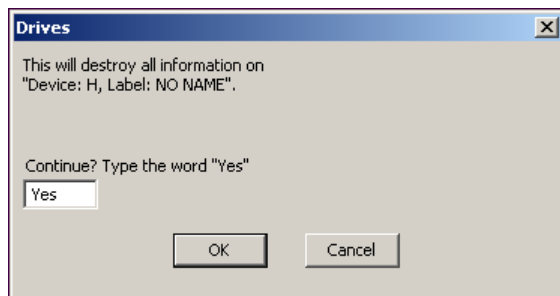
3. Choose the device targeted for erasure and click **Next**.

An options dialog displays. The **Verify wiped sectors** box is checked by default and the **Wipe character** is hex 00. If the box is checked, the Wipe Drive program reads each sector and verifies that the wipe character is written throughout. You can enter any hex value in the Wipe character field.



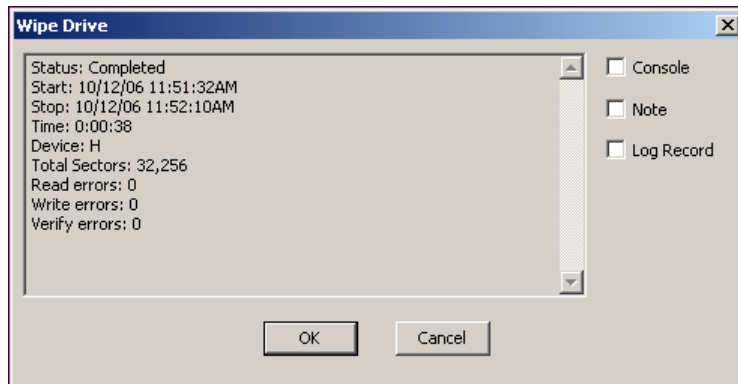
4. Click **Finish**.

The Drives dialog opens:



5. Enter "Yes" in the Continue box and click **OK**.

The drive is completely erased and overwritten with the specified hex string. **Wipe Drive** displays information about the disk and the operation.



You must reformat this drive in order to use it again.

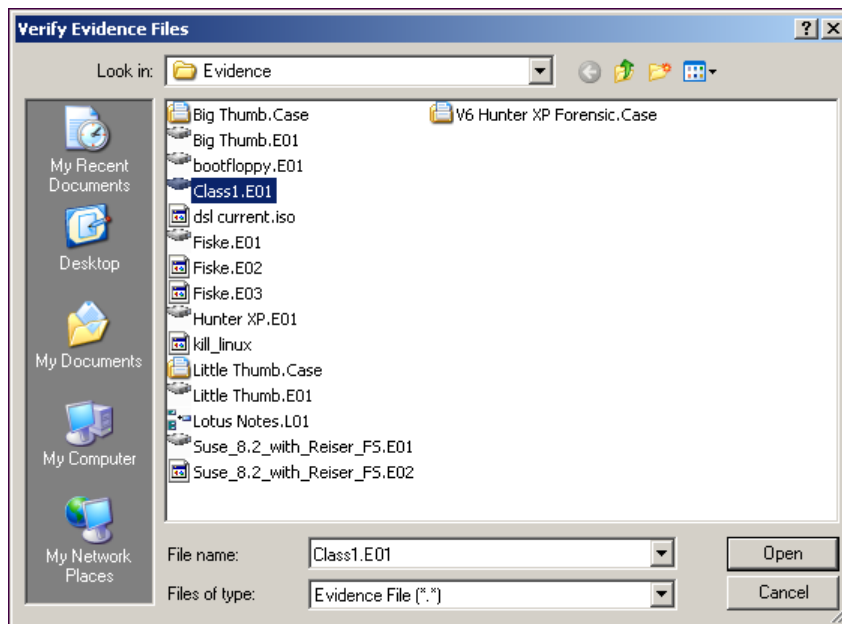
## Verifying Evidence Files

Verify Evidence Files checks CRC values of selected files. It is a way to ensure that evidence is not tampered with. Verified CRC information is written out to a log file. If a CRC verification fails, a notification appears and you can log the error to the console, bookmark tab, or log file.

Acquire the evidence files.

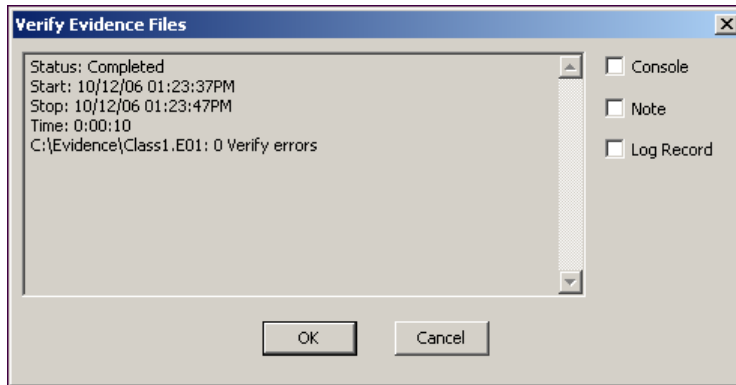
1. Click **Tools > Verify Evidence Files**.

The Verify Evidence Files file browser appears.



2. Select one or more evidence files and click **Open**.

When files are verified, a status report appears.



## Creating a LinEn Boot Disc

You have a copy of a Linux distribution.

See *Creating a LinEn Boot Disc* (on page 47) for more information.



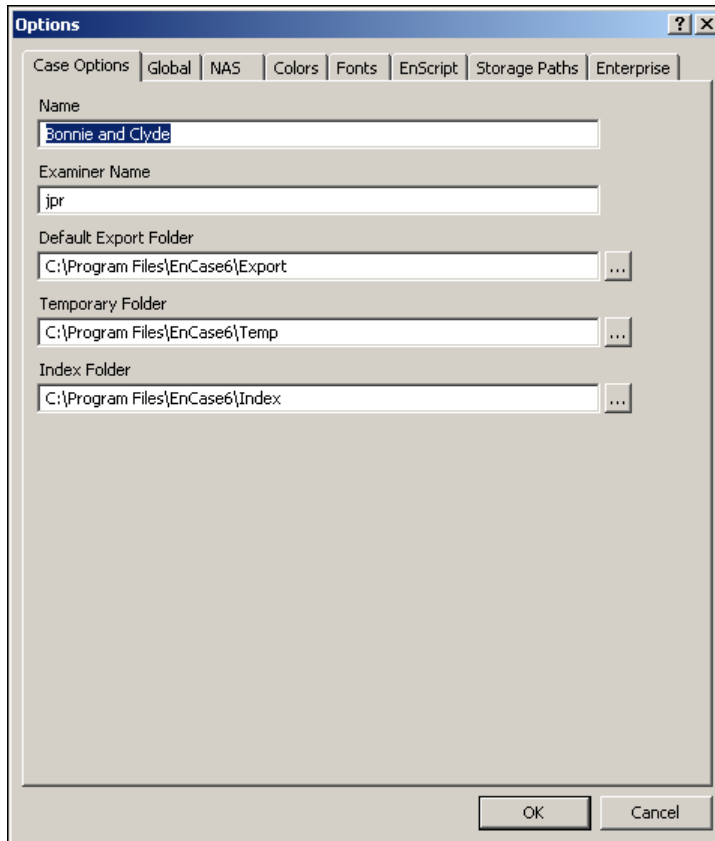
## Options

Use the Options dialog to customize the software.

See the chapter *The Options Dialog* (on page 155) for complete information on this topic.

1. Click **Tools > Options**.

The Options dialog opens.



2. Click on a tab to make changes to settings.
3. When you are finished making the changes to tabs, click **OK**.



# Glossary of Terms



## Glossary of Terms

### A

#### ASCII

ASCII ( American Standard Code for Information Interchange) is a character encoding based on the English alphabet. ASCII codes represent text in computers, communications equipment, and other devices that work with text. Most modern character codes have a historical basis in ASCII. ASCII was first published as a standard in 1967 and was last updated in 1986. It currently defines codes for 33 non-printing, mostly obsolete control characters that affect how text is processed, plus 95 printable characters.

### B

#### Bookmark

Bookmarks let you annotate evidence and analytical artifacts. Files, folders, address ranges within files, collections of files or data, and even bookmarks themselves can be book marked.

#### Burn

The process of recording data to an optical disc, such as a CD or DVD.

### C

#### Case File

A text file containing information specific to one case. The file includes pointers to one or more evidence files, devices, bookmarks, search results, sorts, hash analysis results, and signature analysis.

#### Checksum

A form of redundancy check for protecting the integrity of data by detecting errors. It works by adding the basic components of a message (typically the asserted bits) and storing the resulting value. Later, anyone can perform the same operation on the data, compare the result to the authentic checksum, and, if the sums match, conclude that the data was not corrupted. A major drawback to checksum is that 1234 generates the same check as 4321.

#### Cluster

A cluster is the smallest amount of disk space that can be allocated to hold a file.

#### Code Page

A code page interprets a series of bits as a character.

#### Compound File

A file containing other file types within it. For example, a Microsoft Word file can contain text, graphics, and spreadsheet files.

#### Computer Forensics

The application of scientific method to digital media to establish factual information for judicial review. This process often involves investigating computer systems to determine whether they were used for illegal or unauthorized activities.

#### Connection

The communications between the servlet and the client occur across a connection. This connection may involve communicating through the SAFE.

### Cyclical Redundancy Check (CRC)

The CRC is a variation of the checksum. Its advantage is that it is order sensitive. The string "1234" and "4321" produces the same checksum, but not the same CRC.

## D

### Device Configuration Overlay (DCO)

The Device Configuration Overlay (sometimes called Disk Configuration Overlay) is similar to the Host Protected Area. It is an optional feature within the ATA-6 standard and is supported by most hard disks. Like the HPA, it can also be used to segment a portion of the hard disk drive capacity from view by the OS or file system, usually for diagnostic or restoration purposes.

### Disk Slack

This is the area between the end of the volume and the end of the device.

## E

### EnCase® Forensic

EnCase Forensic is recognized as the standard computer forensic software used by more than 15,000 investigators and 40 of the Fortune top 50 companies. EnCase Forensic provides law enforcement, government and corporate investigators reliable, court-validated technology trusted by leading agencies worldwide since 1997.

### Encryption

The process of encoding information to make it unreadable without a key to decode it.

### EnScript® Language

A programming language and Application Program Interface (API) that has been designed to operate within the EnCase environment.

### Evidence File

The central component of the EnCase methodology is the evidence file. This file contains three basic components (header, checksum, and data blocks) that work together to provide a secure and self-checking description of the state of a computer disk at the time of analysis.

### Examiner

A general destination folder to place data copied from the evidence folder.

### Export Folder

A general destination folder to place data copied from the evidence file.

## F

### FastBloc®

FastBloc is a collection of hardware write-blockers and one software write blocker.

### File Allocation Table (FAT)

Refers to a file system used primarily in DOS and Windows operating systems. There are several levels designed to cope with larger devices. FAT12 is usually used for removable media, whereas FAT16 was initially used on hard drives. FAT16 has a 2GB size limit, so FAT32 was introduced for larger hard drives. FAT32 has been superseded by the New Technology File System (see NTFS) and is the recommended file system for Windows 2000 and later.

### File Signature

Unique identifiers published by the International Standards Organization and the International Telecommunications Union, Telecommunication Standardization Sector (among others) to identify specific file types.

### File Slack

The area between the end of a file and the end of the last cluster or sector used by that file. This area is wasted storage, so file systems using smaller clusters utilize disk space more efficiently.

### Filter Pane

The Filter pane is typically located in the lower-right quadrant of the four pane display. It provides access to EnScript programs, filters, conditions, and queries. (Also see Tree Pane, View Pane, and Table Pane.)

### Font

A coordinated set of glyphs designed with stylistic unity. A font usually comprises an alphabet of letters, numerals, and punctuation marks.

## G

### Globally Unique Identifier (GUID)

A **GUID** is a pseudo-random number used in software applications. While each generated GUID is not guaranteed to be unique, the total number of unique keys ( $2^{128}$  or  $3.4 \times 10^{38}$ ) is so large that the probability of the same number being generated twice is exceptionally small.

### GREP

An acronym for search **G**lobally for lines matching the **R**egular Expression, and **P**rint them.

GREP is a command line utility originally written for use with the Unix operating system. The default behavior of GREP takes a regular expression on the command line, reads standard input or a list of files, and outputs the lines containing matches for the regular expression. The GREP implementation in EnCase has a smaller subset of operators than GREP used in Unix.

### GUID

See Globally Unique Identifier.

## H

### Hash

A method used to generate a unique identifier for the data the hash value represents. There are several standardized hashing algorithms. EnCase uses the 128-bit MD5 hashing algorithm which has  $2^{128}$  unique values. This ensures that the chance of finding an identical hash value using a different data set is exceptionally small.

### Hash Sets

Collections of hash values for groups of files.

### Hexadecimal

A numeral system with a radix or base of 16 usually written using the symbols 0-9 and A-F or a-f. For example, the decimal numeral 79 whose binary representation is 01001111 can be written as 4F in hexadecimal (4 = 0100, F = 1111).

## Host Protected Area (HPA)

An area of a disk designed to allow vendors to store data safe from user access, diagnostics, or backup tools. If present, data stored in this area is inaccessible by the operating system, BIOS or the disk itself.

## I

### Index

An EnCase index is a feature that allows quick access to the data in an evidence file.

### Internet Protocol Address (IP)

A unique number that devices use to identify and communicate with each other on a computer network utilizing the Internet Protocol standard. Any participating network device, including:

- routers
- computers
- time-servers
- printers
- Internet fax machines
- some telephones - must have its own unique address.

An IP address can also be thought of as the equivalent of a street address or a phone number.

IPv4 specifies addresses in four eight-bit decimal numbers separated by a dot. IPv4 specifies a port number with a colon.

IPv6 addresses the limitations that IPv4 has with the total number of addresses. IPv6 is typically written in eight 16-bit hexadecimal numbers, which are separated by a colon. IPv6 specifies a port number with a space.

## K

### Keyword

A keyword is a string or expression used in searching your evidence.

## L

### LinEn Utility

The Linux EnCase client used for disk-to-disk or cable acquisitions.

### Logical Evidence File

A specialized form of an evidence file filled with user-selectable files, as opposed to a traditional evidence file which contains the entire contents of the device. Logical Evidence files have the extension .L01.

## M

### Malware

Software designed to infiltrate or damage a computer system without the owner's informed consent.

### Mount, Mounting

The process of making a file system ready for use by the operating system, typically by reading certain index data structures from storage into memory ahead of time. The term recalls a period in the history of computing when an operator had to mount a magnetic tape or hard disk on a spindle before using it.

## N

### Network Tree

The network tree represents the hierarchical organization of the underlying network and file structure.



**New Technology File System (NTFS)**

The standard file system of Windows NT and its descendants:

- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista

**Node**

A node is the machine where the servlet is installed.

**Notable File Bookmarks**

Bookmarks used to identify individual files containing important information to a case.

**NTFS**

See New Technology File System.

**P****Pane**

Panes comprise the four quadrants to the interface:

- Tree pane
- Table pane
- View pane
- Filter pane

Panes contain tabs, which alter the display of the data inside the pane. Panes are resizable.

**Physical Disk Emulator (PDE)**

The EnCase Physical Disk Emulator lets examiners mount computer evidence as a local drive for examination in Windows Explorer. This feature allows examiners many options in their examinations, including the use of third-party tools with evidence served by EnCase.

**Port**

A virtual data connection that can be used by programs to exchange data directly, instead of going through a file or other temporary storage location. The most common of these are TCP and UDP ports used to exchange data between computers on the Internet

**R****Redundant Array of Independent Disks (RAID)**

A data storage scheme using multiple hard drives to share or replicate data among the drives. Depending on the configuration of the RAID (typically referred to as the RAID level), the benefits of RAID are:

- increased data integrity
- fault-tolerance
- throughput or capacity compared to single drives

**Regular Expression**

A string that describes or matches a set of strings according to certain syntax rules. Many text editors and utilities use regular expressions to search and manipulate bodies of text based on certain patterns. Many programming languages support regular expressions for string manipulation. Also see GREP.

**Root**

The base of a file system's directory structure or the parent directory of a given directory.

## S

### Sector

A subdivision of a track of a magnetic hard disk or optical disc. A sector stores a fixed amount of data. A typical sector contains 512 bytes.

### Secure Authentication For EnCase (SAFE)

The SAFE (Secure Authentication For EnCase) is a physically and logically secured server that authenticates all users and controls all access to the network devices.

### Security Key

A uniquely programmed hardware key, sometimes referred to as a dongle, that identifies a user to EnCase software and enables access to its features.

### Servlet

Servlets are EnCase services running on network workstations and servers that provide bit-level access to the machine where they reside.

### Signature

See File Signature.

### Slack

See Disk Slack and File Slack .

### Snapshot

A representation of a live running machine, including volatile computer data such as currently logged on users, registry settings, and open files.

## Spyware

Refers to a broad category of malicious software designed to intercept or take partial control of a computer without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

## Steganography

The art and science of writing hidden messages in a way that no one except the intended recipient knows of the existence of the message; this is in contrast to cryptography, which does not disguise the existence of the message but obscures its content.

## Subject

The computer or media that the investigator actually examines.

## Swap File

A memory management technique where non-contiguous memory is presented to a software process as contiguous memory. Memory pages stored in primary storage are written to secondary storage, thus freeing faster primary storage for other processes in use. A swap file is also called a page file.

## T

### Table Pane

Part of the program user interface located in the upper-right quadrant of the four pane display.

**Temp Folder**

A folder that allows segregation and control of temporary files created in the course of an investigation. Also see Export Folder.

**Tree Pane**

A part of the program user interface located in the upper-left quadrant of the four pane display.

**U****Unicode**

An industry standard that enables text and symbols from all the world's writing systems to be consistently represented and manipulated by computers. Unicode consists of:

- A character repertoire
- An encoding methodology and set of standard character encoding
- A set of code charts for visual reference
- An enumeration of character properties such as upper and lower case
- A set of reference data computer files
- Rules for normalization, decomposition, collation and rendering

**V****View Pane**

A part of the program user interface located in the lower-left quadrant of the four pane display.

**Virtual File System (VFS)**

The EnCase Virtual File System (VFS) lets examiners mount computer evidence as a read-only, offline network drive for examination in Windows Explorer. The value of this feature is that it allows examiners multiple examination options, including the use of third-party tools with evidence served by EnCase.

**Virtual Machine**

Software that creates a virtual environment on a computer platform so the user can run software. Several discrete execution environments reside on a single computer, each running an Operating System. This allows applications written for one OS to run on a machine with a different OS.

**VMWare**

A wholly-owned subsidiary of EMC Corporation, it supplies much of the virtualization software available for x86-compatible computers. VMWare software runs on Windows and Linux.

**W****Write Blocker**

A tool (software or hardware) that prevents writes to a subject device while allowing investigators to safely read from the device.



# Guidance Software

- Legal Notification 535
- Support 537

## Legal Notification

CEIC, EnCase eDiscovery Suite, EnCase Enterprise, EnCase Enterprise AIRS, EnCase Forensic, EnCE, EnScript, FastBloc, Guidance Software, Neutrino, Snapshot, and WaveShield are registered trademarks or trademarks owned by Guidance Software in the United States and other jurisdictions and may not be used without prior written permission. All other marks and brands may be claimed as the property of their respective owners. Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation into the owners' benefit, without intent to infringe.

Any use and duplication of this material is subject to the terms of the license agreement between you and Guidance Software. Except as stated in the license agreement or as otherwise permitted under Sections 107 or 108 of the 1976 United States Copyright Act, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise.

Product Manuals and Documentation are specific to the software versions for which they are written. For previous or outdated manuals, product release information, contact Guidance Software at <http://www.guidancesoftware.com> (<http://www.guidancesoftware.com>).

Specifications and information contained in this manual are furnished for informational use only, and are subject to change at any time without notice.

Protected by U.S. Patent Nos. 7,168,000 and 6,792,545. Patents Pending in the U.S. and other countries.

## Support

Guidance Software develops solutions that search, identify, recover, and deliver digital information in a forensically sound and cost-effective manner. Since our founding in 1997, we have moved into network-enabled investigations, enterprise-wide integration with other security technologies.

This section provides information on our support for you through:

- Reference manuals and release notes
- Support portal on the Web, including access to downloads
- Technical Support Department
- Customer Service Department
- Message Boards
- Training
- Professional Services

## Reference Manuals and Release Notes

Guidance Software provides printed manuals for all of our product line, as well as PDF versions of interim updates and Release Notes describing the new features and problems fixed.

Read this manual to understand the product and its use. Before acquiring live evidence, run several test acquisitions and try different processes for examining files.

## Technical Support

Guidance Software provides a variety of support options, including phone, e-mail, online submission forms, an up-to-date knowledge base, and a message board (technical forum).

Support is available from Sunday, 7:00 PM through Friday, 6:00 PM Pacific Time (Monday, 3:00 AM to Saturday, 1:00 PM GMT). This excludes public holidays in the United States and the United Kingdom during respective business hours.

### Phone/mail support

#### US Contact Info:

215 North Marengo Avenue  
Suite 250  
Pasadena, CA 91101  
Phone: 1-626-229-9191, Option 4  
Fax: 626-229-9199

#### UK Contact Info:

Thames Central, 5th Floor  
Hatfield Road  
Slough, Berkshire UK SL1 1QE  
Phone: +44 (0) 1753552252, Option 4  
Fax: +44 (0) 1753552232

#### Toll-Free Numbers:

Germany: 0-800-181-4625  
China: 10-800-130-0976  
Australia: 1-800-750-639  
Hong Kong: 800-96-4635  
New Zealand: 0-800-45-0523  
Japan: 00-531-13-0890

### Online support

Guidance Software offers a Support Portal to our registered users, providing technical forums, a knowledge base, a bug tracking database, and an Online Request form. The Portal gives you access to all support-related issues in one site. This includes:

- User, product, Beta Testing, and foreign language forums (message boards)
- Knowledge Base
- Bug Tracker
- Technical Services Request Form

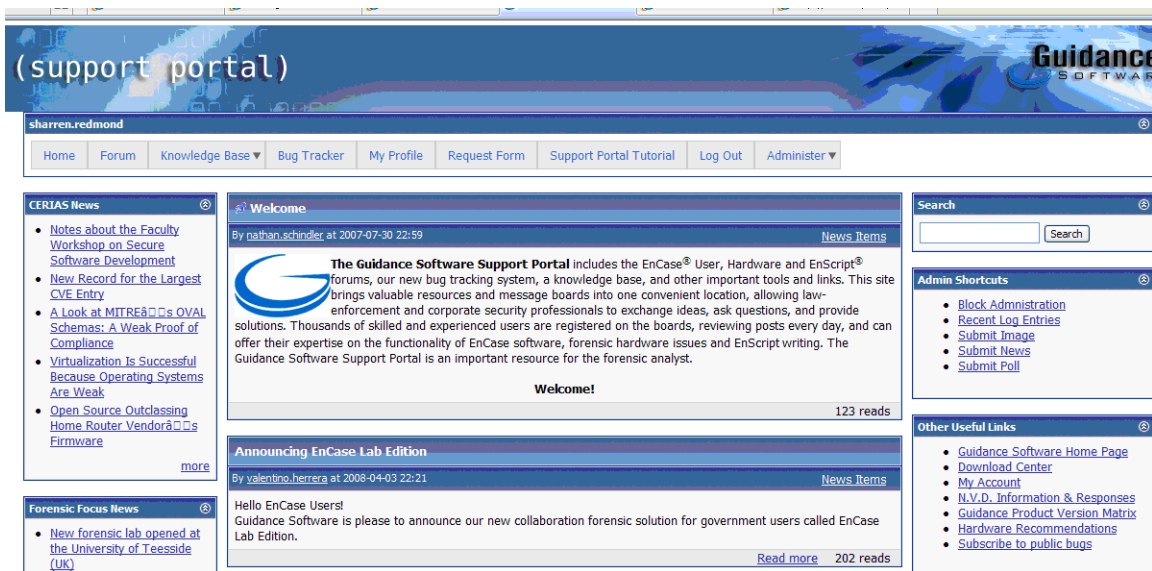


- Downloads of previous software versions, drivers, etc.
- Other Useful Links

Although technical support is available by e-mail, you will receive more thorough, quicker service when you use the online **Technical Support Request Form**

<https://support.guidancesoftware.com/node/381>. Note that all fields are mandatory, and filling them out completely reduces the amount of time it takes to resolve an issue.

If you do not have access to the Support Portal, please use the **Support Portal registration form** <https://support.guidancesoftware.com/forum/register.php?do=signup>.



## Registration

Registration requires you to choose a unique username and password. Please provide all requested information, including dongle ID, phone, e-mail address, organization, etc. This helps us identify you as a registered owner of EnCase.

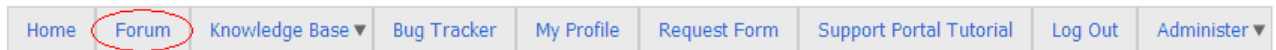
You will receive an email within 24 hours. You must follow the link in that email before you can post on the forums. Until you do that, you will not have permission to post. Once you have verified your email address, you will be added to the Registration List. Please allow 24 business hours for your account to be approved.

Once your registration is approved you can access the **Support Portal** <https://support.guidancesoftware.com/>. You can use the Support Portal Tutorial for a brief overview of the site.



## User, product, and foreign language forums

To access the forums, click on the **Forum Tab** <https://support.guidancesoftware.com/forum/> in the Support Portal.



The forums allow registered users to post questions, exchange information, and hold discussions with Guidance Software and other users in the EnCase community. Different discussion groups are available as follows:

### Foreign Language Groups

- French
- Arabic
- German
- Spanish
- Japanese
- Chinese
- Korean

### Forum Groups

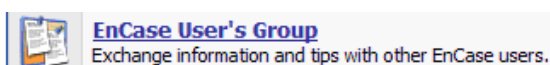
- User Group
- Consultant and Practitioners
- Computer Forensic Hardware Issues
- EnScript Forum

### Product Specific Groups

(only available to customers who have purchased the respective products)


- Neutrino
- Enterprise
- FIM
- eDiscovery

Enter a Group by clicking on the Group name.



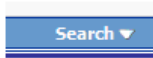
## Posting to a Group

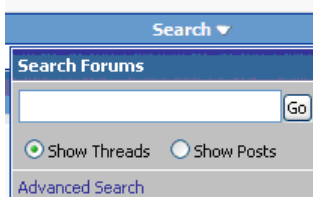
To create a new post, click the  icon.

Click the  icon to reply to a post, or use the Quick Reply icon at the bottom of each post.



## Searching

The forums contain an accumulation of over ten years of information. Use the  button to search for keywords, or click Advanced Search for more specific search options.



Search ▼

Search Forums

Go

☒ Show Threads ☐ Show Posts

[Advanced Search](#)

## Bug Tracker

Use Bug Tracker to submit and check the status and priority of submitted defect and enhancement requests. It is broken down by product, showing the current number of bugs/enhancements and public bugs for each product. To access the Bug Tracker, click on the **Bug Tracker tab** <https://support.guidancesoftware.com/forum/project.php> in the Support Portal.

<a href="#">Home</a>	<a href="#">Forum</a>	<a href="#">Knowledge Base ▼</a>	<a href="#">Bug Tracker</a>	<a href="#">My Profile</a>	<a href="#">Request Form</a>	<a href="#">Support Portal Tutorial</a>	<a href="#">Log Out</a>	<a href="#">Administer ▼</a>
<a href="#">EnCase Forensic</a>		<a href="#">Bugs</a>	100	04-30-2008				
		<a href="#">Features</a>	45					
		<a href="#">Public Bugs</a>	169	12:17 AM				

## Knowledge Base

You can find answers to Frequently Asked Questions (FAQs) and other useful product documentation in the Knowledge Base. You can also submit your own articles to help other EnCase users.

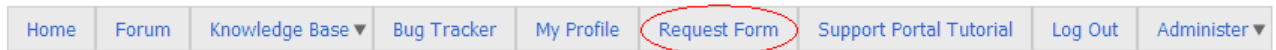
To access the Knowledge Base, click on the **Knowledge Base tab** <https://support.guidancesoftware.com/directory> in the Support Portal.

<a href="#">Home</a>	<a href="#">Forum</a>	<a href="#">Knowledge Base ▼</a>	<a href="#">Bug Tracker</a>	<a href="#">My Profile</a>	<a href="#">Request Form</a>	<a href="#">Support Portal Tutorial</a>	<a href="#">Log Out</a>	<a href="#">Administer ▼</a>
----------------------	-----------------------	----------------------------------	-----------------------------	----------------------------	------------------------------	---	-------------------------	------------------------------

From here, you can browse, search, and write Knowledge Base articles.

### Online Technical Support Request Form

Please use the Technical Support Request Form to request assistance from a Technical Services engineer. To access the form, click on the **Technical Support Request Form** <https://support.guidancesoftware.com/node/381> in the Support Portal.



### Other useful links



The Support Portal's landing page contains a section of useful links, including:

- Guidance Software Home Page
- Download Center: download software, hardware, manuals, boot disks, support articles, etc.
- My Account: register your dongle id to receive up to date software by email
- NVD (National Vulnerability Database) Information and Responses
- Guidance product Version Matrix: check compatibility of different product versions
- Hardware Recommendations: hardware recommendations for EnCase Forensic and EnCase Enterprise
- Subscribe to Public Bugs

## Customer Service

The Guidance Software Customer Services Department is staffed by highly-trained, friendly staff capable of resolving any problem regarding your order.

Hours and contact information are listed below.

Phone: 626.229.9191

Fax: 626.229.9199

Email: [customerservice@guidancesoftware.com](mailto:customerservice@guidancesoftware.com)

Internet: [http://www.guidancesoftware.com/support/cs\\_requestform.aspx](http://www.guidancesoftware.com/support/cs_requestform.aspx)

Hours: Monday through Friday 6:00 a.m. to 5:00 p.m., Pacific Time

## Training

Guidance Software offers a variety of professional courses for the beginner, intermediate and advanced user of all its applications. In addition to providing a solid grounding in our software, we also provide our students with accepted best practices for investigation, report generation and evidence preservation.

Guidance Software offers courses for law enforcement agencies, organizations concerned with forensics and incident response, and advanced topics for all users.

## Professional Services

The Guidance Software Professional Services Division (PSD) combines world-leading computer investigations experts with world-leading forensic technology to deliver turnkey solutions to forensic investigations.

Guidance Software has combined its industry-leading computer investigation technology with a team of the most highly trained and capable investigators in the world to bring you complete turnkey solutions for your business. When you face investigative issues that go beyond your internal capabilities, our professional services group is able to respond either remotely or by coming on site to provide the right technology and computer investigations personnel for the job.

### Internal Investigations

- Theft of intellectual property
- Intrusion reconstruction
- Wrongful termination suit

### Compliance

- Sarbanes-Oxley
- PII risk assessment
- California SB 1386

### eDiscovery

- Pending litigation
- Responsive production
- Forensic preservation

### Information Security

- Compromise of system integrity
- Policy review
- Unauthorized use
- Forensic lab implementation

# Index

## 6

64-Bit EnCase Servlet • 19

## A

Acquiring • 193

Acquiring a Disk Running in Direct ATA Mode  
• 53, 215

Acquiring a DriveSpace Volume • 227

Acquiring a Local Drive • 209

Acquiring a Palm Pilot • 215

Acquiring Device Configuration Overlays  
(DCO) and Host Protected Areas (HPA) • 53,  
210

Acquiring Disk Configurations • 221

Acquiring Firefox Cache in Records • 228

Acquiring in Windows Without a FastBloc Write  
Blocker • 213

Acquiring Non-local Drives • 219

Acquiring SlySoft CloneCD Images • 226

Acquiring Virtual PC Images • 226

Acquisition Results Dialog • 202

Acquisition Times • 219

Acquisition Wizard • 194, 366

Add Device • 166

Add Device Wizard • 182

Add Note Bookmark Dialog • 404

Adding a Device • 188, 189

Adding a File Viewer to Your EnCase  
Application • 288, 290

Adding a New File Signature • 327

Adding Keywords • 340, 343

Adding Partitions • 247

Adding Raw Evidence Files • 230

Additional WinEn Information • 270

After Acquisition Page • 195

Alternative Report Method • 443

America Online .art Files • 310

Analyzing and Searching Files • 323, 490

AND/OR Filter Logic • 135

App Descriptors • 372

ASCII • 519

Associating Code Pages • 471

Associating the File Viewer's File Types with the  
Viewer • 288, 291

Authentication • 381

Auto Fit • 76

Auto Fit All Columns • 125

## B

Bookmark • 519

Bookmark Content Data Types • 400

Bookmark Data Dialog for Files • 406

Bookmark Data Dialog for Highlighted Data  
Bookmarks • 400

Bookmark Editing Dialogs • 417

Bookmark Features • 399

Bookmark Folder Information/Structure Dialog •  
405

Bookmark Reports and Reporting • 428

Bookmarking an Image • 315

Bookmarking Items • 358, 395

Bookmarking Non-English Language Text • 469

Bookmarks Overview • 395

Booting the Restored Hard Drive • 254

Browse for Folder Dialog • 159, 161

Building a Package • 503

Burn • 519

## C

Canceling an Acquisition • 209

Case Backup • 154

Case File • 519

Case File Format • 153

Case File Time Zones • 169

Case Management • 151, 152

Case Options Page of the New Case Wizard •  
166

Case Options Tab • 32

Case Processor • 485

Case Processor Modules • 487

Case Related Features • 156

CD-DVD Inspector File Support • 226

Changing Filter Order • 135

Changing Report Size • 440

Checksum • 519

Choose Devices Page of the Add Device Wizard  
• 187

Choosing Database Sources • 257

Cleaning an EDB Database • 300

Clearing the Invalid Image Cache • 317

Close Case • 175

Cluster • 519

Code Page • 519

Color Tab • 35

COM Folder EnScript Code • 492

Combining Filters • 134

Command Line Options • 267

- Completing the After Acquisition Page of the Acquisition Wizard • 205
- Completing the Choose Devices Page • 192
- Completing the Destination Page • 286
- Completing the File Selection Page • 285
- Completing the Options Page • 286
- Completing the Options Page of the Acquisition Wizard • 208
- Completing the Preview Devices Page • 192
- Completing the Search Page of the Acquisition Wizard • 206
- Completing the Sessions Sources Page • 191
- Completing the Sources Page • 190
- Compound File • 519
- Compound Files • 489
- Comprehensive Internet History Search • 350
- Computer Forensics • 520
- Concurrent Case Management • 152
- Conditions • 138
- Configuration File • 269
- Configuration File Notes • 270
- Configuring Interface Elements to Display Non-English Characters • 460
- Configuring Non-English Language Support • 459
- Configuring the Keyboard for a Specific Non-English Language • 461
- Configuring Your EnCase Application • 30
- Configuring Your Linux Distribution • 47
- Connection • 520
- Contract All • 117
- Copy • 148
- Copy and Unerase Features • 275
- Copy Folders Dialog • 282, 288
- Copy/UnErase • 64
- Copy/UnErase Wizard • 276
- Copying a Table Entry into a Folder • 425, 426
- Copying and Unerasing Bookmarks • 286
- Copying and Unerasing Files • 284
- Copying and Unerasing Files and Folders • 275
- Copying Folders • 287
- Create a Hash Set • 336
- Create an App Descriptor with an EnScript Program • 374
- Create License Dialog • 501
- Create Logical Evidence File Wizard • 239
- Creating a Bookmark • 407, 415
- Creating a Datamark as a Bookmark • 415
- Creating a File Group Bookmark • 412
- Creating a Filter • 130

- Creating a Folder Information/Structure Bookmark • 410
- Creating a Highlighted Data Bookmark • 408
- Creating a License • 503
- Creating a LinEn Boot Disc • 46, 514
- Creating a Log Record Bookmark • 413
- Creating a Logical Evidence File • 242
- Creating a Notable File Bookmark • 411
- Creating a Notes Bookmark • 409, 415
- Creating a Package • 502
- Creating a Report Using Case Processor • 449
- Creating a Report Using the Report Tab • 437
- Creating a Snapshot Bookmark • 414
- Creating a Webmail Report • 442
- Creating an Additional Fields Report • 447
- Creating and Defining a New Text Style • 463
- Creating Conditions • 139
- Creating Global Keywords • 339
- Creating International Keywords • 342
- Creating Non-English Keywords • 465
- CREDANT Encryption Support (File-Based Encryption) • 384
- CREDANT Encryption Support (Offline Scenario) • 387
- Customer Service • 534
- Customizing a Report • 415, 428, 430
- Cyclical Redundancy Check (CRC) • 520

## D

- Datamarks • 399
- Dates • 402
- Decrypted Block • 320
- Deleting a Filter • 137
- Deleting Items • 128, 357
- Deleting Partitions • 249
- Destination Page of the Copy/UnErase Wizard • 281
- Determining Local Mailbox Encryption • 318
- Device Configuration Overlay (DCO) • 520
- Disabling Microsoft Windows Vista User Account Control • 41
- Disk Configuration Set Acquired as One Drive • 224
- Disk Configurations Acquired as Separate Drives • 225
- Disk Encryption Support • 378
- Disk Slack • 520
- Displaying Expanded Tree Entry Information • 119



Displaying Tree Entry Information for One Branch • 118  
 Document Incident • 476  
 Doing a Crossover Cable Preview or Acquisition • 55  
 Doing a Drive-to-Drive Acquisition Using LinEn • 51  
 Doing a Typical Acquisition • 194  
 Dynamic Disk • 223

## E

Edit Bookmark Folder Dialogs • 422  
 Edit Datamarks Dialog • 421  
 Edit Folder Dialog • 423  
 Edit Folder Information/Structure Bookmarks Dialog • 419  
 Edit Highlighted Data Bookmarks Dialog • 418  
 Edit Log Record Bookmarks Dialog • 421  
 Edit Menu • 63  
 Edit Notable File Bookmarks Dialog • 420  
 Edit Note Bookmarks Dialog • 419  
 Edit SAFE Dialog • 162  
 Edit Snapshot Bookmarks Dialog • 420  
 Editing a Bookmark • 415, 416  
 Editing a Filter • 131  
 Editing a Package • 503  
 Editing a Signature • 328  
 Editing Conditions • 141  
 EFS Files and Logical Evidence (LO1) Files • 393  
 Email Report • 441  
 Enabling or Disabling Entries in the Report • 438, 448  
 Enabling the Forensic Administrator Role on the CREDANT Server • 389  
 EnCase Evidence Files • 178  
 EnCase Examiner Support for Microsoft Vista • 19  
 EnCase® Forensic • 520  
 Encode Preview • 358  
 Encrypted Block • 319  
 Encryption • 520  
 Encryption Support • 375  
 EnScript Analysis • 473, 474  
 EnScript Debugger • 493  
 EnScript Example Code • 492  
 EnScript File Mounter • 496  
 EnScript Help • 498  
 EnScript Programming Language • 333  
 EnScript Programs Shortcut Submenu • 510  
 EnScript Tab • 38

EnScript Types • 334, 498  
 EnScript® Language • 520  
 Entering Non-English Content without Using Non-English Keyboard Mapping • 462  
 Enterprise EnScript Programs • 180, 475  
 Error Handling • 270  
 Evidence File • 520  
 Evidence File Time Zones • 170  
 Examiner • 520  
 Exchange Server Synchronization • 299  
 Exclude File Bookmarks • 431  
 Exclude Files • 128, 355, 357  
 Exclude Folder • 432  
 Excluding Bookmarks • 431  
 Excluding Search Hits • 127  
 Expand All • 116  
 Export Folder • 520  
 Export Keywords • 345  
 Export to \*.msg • 370  
 Exporting a Machine Profile from the SafeBoot Server • 380  
 Exporting a Report • 448  
 Exporting Conditions • 144  
 Exporting Filters • 137  
 Exporting to \*.msg • 370  
 Extracting Email • 366

## F

FastBloc® • 521  
 FAT, HFS and CDFS Time Zone Specifics • 172  
 File Allocation Table (FAT) • 521  
 File Group Bookmarks • 397  
 File Hashing • 335  
 File Menu • 62  
 File Mounter • 488  
 File Selection Page of the Copy/UnErase Wizard • 277  
 File Signature • 521  
 File Signatures • 324  
 File Signatures with Suffixes • 325  
 File Slack • 521  
 File Viewer Features • 288  
 File Viewers • 288  
 Filter Pane • 521  
 Filter Pane Menu • 76  
 Filtering Effects in Table Pane • 94  
 Filters • 129  
 Filters Pane • 93  
 Filters Pane Menu • 105  
 Find • 148  
 Fitting Columns to Data • 125

Folder Information/Structure Bookmarks • 397  
Font • 521  
Fonts Tab of the Options Dialog • 36  
Forensic EnScript Code • 484

## G

Gallery Tab • 146, 314  
General Time Zone Notes • 172  
Generating an Index • 362  
Generating Reports on the Database • 262  
Getting Ready to Acquire the Content of a Device • 180  
Global Tab • 33  
Globally Unique Identifier (GUID) • 521  
Glossary of Terms • 517  
Goto • 148  
GREP • 521  
GUID • 521  
Guidance Software • 527

## H

Hardware Disk Configuration • 224  
Hash • 522  
Hash a New Case • 335  
Hash Analysis • 334  
Hash Sets • 336, 522  
Hashing • 236  
Hashing the Subject Drive Once Previewed or Acquired • 237  
Hashing the Subject Drive Using LinEn • 57, 236  
Help for EnScript Modules • 495  
Help Menu • 78  
Hexadecimal • 522  
Hiding Columns • 124  
Highlighted Data Bookmarks • 396  
Host Protected Area (HPA) • 522

## I

If the Restored Disk Does Not Boot • 255  
Import Keywords • 345  
Importing Conditions • 143  
Importing Filters • 137  
Include EnScript • 497  
Included Enscript Components • 333  
Increasing the Number of Images Per Row • 316  
Index • 522  
Index Case • 490  
Indexing • 152, 360  
Indexing a Case • 152

Individual Panes • 88  
Initializing the Database • 256  
Installed Files • 25  
Installing EnCase Forensic • 21  
Installing Security Keys • 29  
Installing the Examiner • 23  
Integers • 402  
Internet History Searching • 350  
Internet Protocol Address (IP) • 522  
Internet Report • 442  
Internet Searching • 351  
Introduction • 15, 45

## K

Keyword • 522  
Keyword Searches • 339  
Keyword Tester • 343

## L

Leaving Console Mode • 218  
LEF EFS Encryption Enhancement • 17  
Legal Notification • 527  
LinEn Set Up Under Red Hat • 48  
LinEn Set Up Under SUSE • 48  
LinEn Utility • 522  
Live Device and FastBloc Indicators • 181  
Local Keywords • 345  
Locally Encrypted NSF Parsing Results • 321  
Log Record Bookmarks • 398  
Logical Evidence File • 523  
Logical Evidence Files • 178, 238  
Logical Restore • 254  
Logon Wizard • 157  
Logon Wizard Users Page • 158  
Lotus Notes Local Database Encryption • 18  
Lotus Notes Local Encryption Support • 317

## M

Machine Survey Servlet Deploy • 478  
Maintaining the Database • 257  
Malware • 523  
Manually Create App Descriptor • 373  
Minimum Requirements • 22  
Mode Selection • 54  
Modifying Case Related Settings • 167  
Modifying the Table Pane • 122  
Modifying the View Pane • 148  
Mount, Mounting • 523  
Mounting Compound Files • 490

Moving a Table Entry into a Folder Using the Right-Click Drag Method • 425, 427  
 Moving a Table Entry or Folder into a Folder Using the Drag Method • 428

## N

Navigating the EnCase Interface • 59  
 Navigating the Tree Pane • 115  
 Network Tree • 523  
 New Case Wizard • 164  
 New Features • 17  
 New File Viewer Dialog • 289  
 New Package Dialog • 499  
 New Technology File System (NTFS) • 523  
 New Text Styles Dialog • 456  
 New Text Styles Dialog Attributes Tab • 456  
 New Text Styles Dialog Code Page Tab • 458  
 Node • 523  
 Non-English Language Features • 453  
 Notable File Bookmarks • 397, 523  
 Notes Bookmarks • 397  
 NSF Encryption Support • 376  
 NTFS • 523  
 NTFS Compressed Files • 314

## O

Obtaining a Linux Distribution • 48  
 Obtaining Updates • 30  
 Open a Case • 173  
 Opening and Closing Folders with Expand/Contract • 116  
 Opening the Acquisition Wizard • 203  
 Options • 514  
 Options Page • 200  
 Options Page of the Copy/UnErase Wizard • 279  
 Organizing Bookmarks • 425  
 Overview • 177  
 Overview of Case Structure • 151

## P

Package Features • 498  
 Package Panel • 499  
 Packages • 498  
 Pane • 523  
 Pane Features • 86  
 Pane Tab Bar and Pane Tab Bar Menu • 87  
 Panes • 82  
 Panes and their Specific Tabs • 98  
 Panes as Separate Windows • 84  
 Panes in the Analysis Cycle • 83

Parsing a Locally Encrypted Mailbox • 318  
 Performing a Crossover Cable Preview or Acquisition • 219  
 Performing a Drive-to-Drive Acquisition Using LinEn • 213  
 Performing a Search • 352, 366  
 Performing a Signature Analysis • 329  
 Performing Acquisitions with LinEn • 49  
 Physical Disk Emulator (PDE) • 523  
 Physical Restore • 251  
 Physical vs. Logical Restoration • 250  
 Picture • 401  
 Port • 523  
 Preparing the Target Media • 250  
 Preview Devices Page of the Add Device Wizard • 189  
 Previewing • 181  
 Previewing the Content of a Device • 182  
 Professional Services • 535  
 Prompt for Value • 270  
 Properties Panel • 500

## Q

Queries • 145  
 Querying an Index Using a Condition • 361  
 Querying the Index for Non-English Content • 468  
 Quick Entry Report • 446  
 Quick Snapshot • 481

## R

RAID-10 • 226  
 Raw Image Files • 179  
 Reacquiring an Evidence File • 229  
 Reacquiring Evidence • 229  
 Rebuild a Hash Library • 338  
 Recover Folders on FAT Volumes • 244  
 Recovering a Database • 301  
 Recovering Folders • 243  
 Recovering Folders from a Formatted Drive • 246  
 Recovering NSF Passwords • 377  
 Recovering NTFS Folders • 244  
 Recovering Partitions • 246  
 Recovering UFS and EXT2/3 Partitions • 246  
 Reducing the Number of Images Per Row • 316  
 Redundant Array of Independent Disks (RAID) • 524  
 Reference Manuals and Release Notes • 528  
 Regular Expression • 524

- Reinstalling the Examiner • 28
- Remote Acquisition • 231
- Remote Acquisition Monitor • 233, 481
- Repairing a Database • 302
- Report Multiple Files • 439
- Report Single Files • 438
- Reporting • 437
- Resetting Columns • 125
- Restoring Evidence • 250
- Role Page of the New Case Wizard • 165
- Root • 524
- Running a 32-bit Application on a 64-bit Platform • 43
- Running a Filter • 132
- Running a Package • 504
- Running Conditions • 142
- Running WinEn • 267

## S

- S/MIME Encryption Support • 389
- SAFE Page of the Logon Wizard • 160
- SAFE Right-Click Menu • 160
- SafeBoot Encryption Support (Disk Encryption) • 381
- SafeBoot Setup • 379, 380
- Saving a Case • 174
- Saving a Case and the Global Application Files • 174
- Saving a Case With a New Name or New Location • 174
- Scan Local Machine • 490
- Search Hits Report • 444
- Search Options • 352
- Search Page • 197
- Searching Email • 366, 368
- Searching Entries for Email and Internet Artifacts • 347
- Searching for Email • 364, 366
- Searching Selected Items • 368
- Sector • 524
- Secure Authentication For EnCase (SAFE) • 524
- Security Key • 524
- Selecting Tree Entries for Operations • 120
- Send to HBGary Responder EnScript • 19
- Send To HBGary Responder EnScript • 504
- Servlet • 524
- Sessions Sources Page of the Add Device Wizard • 185
- Setting a Lock on Columns • 126
- Setting Time Zone Options for Evidence Files • 171
- Setting Time Zones Settings for Case Files • 170
- Setting Up the Storage Machine • 234
- Setup for a Drive-to-Drive Acquisition • 50
- Sharing Configuration Files • 40
- Show Deleted Files • 358
- Show Excluded • 434
- Show Excluded Files • 356
- Showing Columns • 123
- Signature • 524
- Signature Analysis • 146, 314, 324
- Signature Analysis Legend • 332
- Single Files • 179
- Slack • 524
- Snapshot • 524
- Snapshot Bookmarks • 398
- Snapshot Differential Report • 482
- Snapshot to DB Module Set • 18, 255
- Software RAID • 221
- Sorting a Table • 92
- Sources Page • 240
- Sources Page of the Add Device Wizard • 183
- Specifying and Running an Acquisition • 204
- Specifying Database Content • 261
- Spyware • 524
- Status Line • 96
- Steganography • 525
- Storage Paths Tab • 39
- Styles • 403
- Subject • 525
- Support • 528
- Supported Encryption Algorithms • 387
- Supported File Systems and Operating Systems • 179
- Supported SafeBoot Encryption Algorithms • 384
- Swap File • 525
- Sweep Enterprise • 483
- System Menu • 61

## T

- Tab Right-Click Menu • 88
- Table Pane • 91, 525
- Table Pane Menu • 72
- Table Pane Tabs • 99
- Table Tab Columns • 102, 123
- Technical Support • 529
- Temp Folder • 525
- Testing a Non-English Keyword • 467

- Testing an EDB File • 301
- Text • 401
- Text Styles • 455
- The Console Tab • 114
- The Details Tab • 114
- The Doc Tab • 111
- The EnCase Installer • 21
- The Filter Pane and its Tab Bar and View Menu • 75
- The Hex Tab • 110
- The Main Window • 60
- The Options Dialog • 154, 514
- The Options Dialog Font Tab • 454
- The Output Tab • 115
- The Outputs Page of the Create Logical Evidence File • 241
- The Picture Tab • 112
- The Report Tab • 113
- The Table Pane and its Tab Bar and View Menu • 71
- The Text Tab • 109
- The Transcript Tab • 112
- The Tree Pane and its Tab and Sub-Tab Menus • 70
- The View Pane and its Tab Bar and View Menu • 73
- Time Zone Example • 173
- Time Zone Settings • 168
- Timeline Tab • 147
- Toolbar • 80, 508
- Tools Menu • 77, 509
- Training • 534
- Tree Pane • 89, 525
- Tree Pane Tabs • 99
- Troubleshooting Security Keys • 29
- Turning Filters Off • 136
- Turning On Encode Preview • 358
- Types of Acquisitions • 193
- Types of Entries • 178

## U

- Unicode • 525
- Unicode Fonts • 455
- Uninstalling the Examiner • 26
- Updating the Database • 258
- Users Right-Click Menu • 158
- Using a Case • 167
- Using a Folder to Organize a Bookmarks Report • 415, 424, 425
- Using a Package • 502
- Using a Write Blocker • 210
- Using Bookmarks • 415
- Using EnCase Tools • 507
- Using LinEn • 45
- Using Snapshots • 180
- Using the Dixon Box • 121
- Using the Snapshot DB Reports Dialog • 264

## V

- Validating Parity on a RAID-5 • 226
- Verifying Evidence Files • 513
- View Menu • 66
- View Pane • 96, 292, 525
- View Pane Menu • 74
- View Pane Tabs • 106
- Viewer File Type Dialog • 289
- Viewing a Bookmark on the Table Report Tab • 415, 428, 429
- Viewing a Bookmark Report • 440
- Viewing Attachments • 367, 368
- Viewing Base64 and UUE Encoded Files • 312
- Viewing Compound Files • 293
- Viewing Compressed Files • 298
- Viewing Fewer Columns • 146
- Viewing Fewer Rows • 147
- Viewing File Content • 273
- Viewing File Structure • 293
- Viewing Files • 274
- Viewing Hash Search Results • 338
- Viewing Lotus Notes Files • 299
- Viewing Macintosh .pax Files • 307
- Viewing More Columns • 146
- Viewing More Rows • 147
- Viewing MS Exchange Files • 299
- Viewing MS Outlook Email • 306
- Viewing Non-Unicode Files • 471
- Viewing Office 2007 Documents • 310
- Viewing OLE Files • 297
- Viewing Outlook Express Email • 303
- Viewing Record Search Hits • 354
- Viewing Registry Files • 295
- Viewing Search Hits • 355
- Viewing Signature Analysis Results (Part 1) • 330
- Viewing Signature Analysis Results (Part 2) • 331
- Viewing the File Signature Directory • 325
- Viewing the License for LinEn • 46
- Viewing Unicode Files • 470
- Viewing Windows Thumbs.db • 309
- Virtual File System (VFS) • 525
- Virtual Machine • 526

Vista Examiner Support • 40

VMWare • 526

## **W**

Web Mail Parser • 365

Webmail Parser • 491

When to use a Crossover Cable • 219

Windows • 403

Windows NT - Software Disk Configurations •  
222

Windows-based Acquisitions with a non-  
FastBloc Write Blocker • 213

Windows-based Acquisitions with FastBloc  
Write Blockers • 211

WinEn • 18, 266

Wipe Drive • 510

Working with Evidence • 177

Working with Non-English Languages • 403,  
451, 452

Write Blocker • 526